#2

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re the Application of	: **Hideaki NEGAWA**
Filed:	: **Concurrently herewith**
For:	: **MULTICAST COMMUNICATION SYSTEM**
Serial No.	: **Concurrently herewith**

Assistant Commissioner for Patents
Washington, D.C. 20231

December 17, 2001

PRIORITY CLAIM AND

SUBMISSION OF PRIORITY DOCUMENT

S I R:

Applicant hereby claims priority under 35 USC 119 from **JAPANESE** patent application no. **2001-258890** filed **August 29, 2001,** a certified copy of which is enclosed.

Any fee, due as a result of this paper, not covered by an enclosed check, may be charged to Deposit Acct. No. 50-1290.

Respectfully submitted,

Harris A. Wolin
Reg. No. 39,432

ROSENMAN & COLIN, LLP
575 MADISON AVENUE
IP Department
NEW YORK, NEW YORK 10022-2584
DOCKET NO.:FUJH 19.264
TELEPHONE: (212) 940-8800

#2

日 本 国 特 許 庁
JAPAN PATENT OFFICE

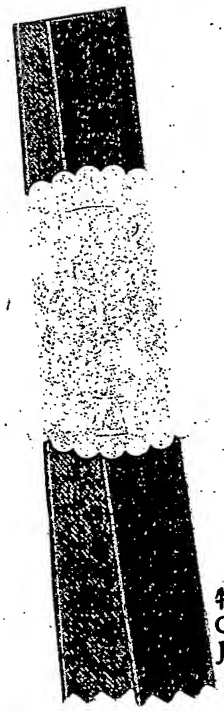
別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００１年 ８月２９日

出願番号
Application Number: 特願２００１－２５８８９０

出願人
Applicant(s): 富士通株式会社



２００１年１０月１９日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造

出証番号 出証特２００１－３０９１４８０

【書類名】　特許願
【整理番号】　0151296
【提出日】　平成13年 8月29日
【あて先】　特許庁長官　殿
【国際特許分類】　H04L 9/00
H04H 1/00
H04L 12/14
【発明の名称】　マルチキャスト通信システム
【請求項の数】　5
【発明者】
【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
【氏名】　子川　英昭
【特許出願人】
【識別番号】　000005223
【氏名又は名称】　富士通株式会社
【代理人】
【識別番号】　100094514
【弁理士】
【氏名又は名称】　林　恒▲徳▼
【代理人】
【識別番号】　100094525
【弁理士】
【氏名又は名称】　土井　健二
【手数料の表示】
【予納台帳番号】　030708
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9704944

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　マルチキャスト通信システム

【特許請求の範囲】

【請求項１】　所定のデータ配信サービスに関するデータをマルチキャストにより送信するマルチキャストサーバと，マルチキャストグループに属し，前記データを受信する複数のクライアントとを有するマルチキャスト通信システムであって，

前記マルチキャストサーバは，

前記データを第１の暗号化鍵により暗号化するデータ暗号部と，

前記データ暗号部により暗号化されたデータを，前記マルチキャストグループに属するクライアントにマルチキャストにより送信するデータ送信部と，

前記第１の暗号化鍵を第２の暗号化鍵により暗号化する鍵暗号部と，

前記鍵暗号部により暗号化された第１の暗号化鍵を，前記マルチキャストグループに属するクライアントのうち，前記データ配信サービスに加入したクライアントにユニキャストにより送信する鍵送信部と，

を備え，

前記複数のクライアントのうち，前記データ配信サービスに加入したクライアントは，

前記鍵送信部により送信される，暗号化された第１の暗号化鍵を受信する鍵受信部と，

前記鍵受信部により受信された，暗号化された第１の暗号化鍵を復号化鍵により復号化する鍵復号部と，

前記データ送信部により送信される，暗号化されたデータを，前記鍵復号部により得られた第１の暗号化鍵により復号するデータ復号部と，

を備えているマルチキャスト通信システム。

【請求項２】　所定のデータ配信サービスに関するデータを第１の暗号化鍵により暗号化するデータ暗号部と，

前記データ暗号部により暗号化されたデータをマルチキャストにより，所定のマルチキャストグループに属するクライアントにマルチキャストにより送信する

データ送信部と，

前記第１の暗号化鍵を第２の暗号化鍵により暗号化する鍵暗号部と，

前記鍵暗号部により暗号化された第１の暗号化鍵を，前記マルチキャストに属するクライアントのうち，前記データ配信サービスに加入したクライアントにユニキャストにより送信する鍵送信部と，

を備えているマルチキャストデータ送信装置。

【請求項３】　マルチキャストにより送信される，所定のデータ配信サービスに関するデータを受信するマルチキャストデータ受信装置であって，

前記データ配信サービスに加入することにより得られる暗号化された第１の暗号化鍵を復号化する鍵復号部と，

前記データ配信サービスに関するデータが前記第１の暗号化鍵により暗号化されたものを受信するデータ受信部と，

前記データ受信部により受信された，暗号化されたデータを，前記鍵復号部の復号化により得られた第１の暗号化鍵により復号化するデータ復号部と，

を備えているマルチキャストデータ受信装置。

【請求項４】　所定のデータ配信サービスに関するデータをマルチキャストにより送信するマルチキャストサーバと，マルチキャストグループに属し，前記データを受信する複数のクライアントとを有するマルチキャスト通信システムであって，

前記マルチキャストサーバは，

前記データを暗号化するためのデータ暗号化鍵を，所定の更新タイミングごとに，該更新タイミング前に有効なデータ暗号化鍵に，該更新タイミング前に有効なデータ暗号化鍵に対応する更新鍵を作用させることにより得られる関係にある，更新タイミング後に有効となるデータ暗号化鍵に更新する鍵更新部と，

前記更新鍵を生成し，または，あらかじめ保持する更新鍵保持部と，

前記データを現在有効なデータ暗号化鍵により暗号化するデータ暗号部と，

前記データ暗号部により暗号化されたデータを，前記マルチキャストグループに属するクライアントにマルチキャストにより送信するデータ送信部と，

前記更新タイミングごとに，更新タイミング後に有効なデータ暗号化鍵に対応

する更新鍵を，該更新タイミング後に有効なデータ暗号化鍵により暗号化する鍵暗号部と，

前記更新タイミングごとに，前記鍵暗号部により暗号化された更新鍵を前記クライアントにユニキャストまたはマルチキャストにより送信する更新鍵送信部と，

を備え，

前記複数のクライアントのうち，前記データ配信サービスに加入したクライアントは，

前記データ送信部により送信される，暗号化されたデータを受信するデータ受信部と，

前記データ受信部により受信される，前記暗号化されたデータを，前記現在有効なデータ暗号化鍵と同一の現在有効なデータ復号化鍵により復号化するデータ復号部と，

前記更新鍵送信部により送信される，暗号化された更新鍵を受信する更新鍵受信部と，

前記更新鍵受信部により受信される，暗号化された更新鍵を，前記現在有効なデータ復号化鍵により復号化する更新鍵復号部と，

前記データ配信サービスへの加入時には，外部から与えられ，その後は，前記更新タイミングごとに，該更新タイミング前に有効なデータ復号化鍵に，該更新タイミング前に有効なデータ復号化鍵による復号化により得られた前記更新鍵を作用させることにより，更新タイミング後に有効なデータ復号化鍵を生成し，前記更新タイミングごとに，前記更新タイミング前に有効なデータ復号化鍵を前記更新タイミング後に有効なデータ復号化鍵に更新するデータ復号化鍵更新部と，

を備えているマルチキャスト通信システム。

【請求項５】　所定のデータ配信サービスに関するデータを暗号化するためのデータ暗号化鍵を，所定の更新タイミングごとに，該更新タイミング前に有効なデータ暗号化鍵に，該更新タイミング前に有効なデータ暗号化鍵に対応する更新鍵を作用させることにより得られる関係にある，更新タイミング後に有効となるデータ暗号化鍵に更新する鍵更新部と，

前記更新鍵を生成し，または，あらかじめ保持する更新鍵保持部と，

前記データを現在有効なデータ暗号化鍵により暗号化するデータ暗号部と，

前記データ暗号部により暗号化されたデータを，所定のマルチキャストグループに属するクライアントにマルチキャストにより送信するデータ送信部と，

前記更新タイミングごとに，更新タイミング後に有効なデータ暗号化鍵に対応する更新鍵を，該更新タイミング後に有効なデータ暗号化鍵により暗号化する鍵暗号部と，

前記更新タイミングごとに，前記鍵暗号部により暗号化された更新鍵を前記クライアントにユニキャストまたはマルチキャストにより送信する更新鍵送信部と，

を備えているマルチキャストデータ送信装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は，マルチキャスト通信システムに関し，具体的には，所定のデータ配信サービスに関するデータをマルチキャストにより通信するマルチキャスト通信システムに関する。また，本発明は，マルチキャストデータ送信装置およびマルチキャストデータ受信装置に関する。

【０００２】

【従来の技術】

インターネットまたはイントラネットにおいて，多数のクライアント（マルチキャストグループに属するクライアント）に同じデータを配信する周知の技術として，ＩＰマルチキャスト（IP Multicast）がある。このＩＰマルチキャストは，インターネットまたはイントラネット上で音楽，映像等のデータ（コンテンツ）を配信するのに適している。今後，コンテンツの配信にＩＰマルチキャストの利用が盛んになれば，クライアントに対して課金を行い，データ配信サービス料（受信料）を徴収したいという要望が生まれることが予測される。

【０００３】

その際に，課金を適切に行うために，ＩＰマルチキャストグループに属するク

ライアントのうち，データ配信サービスに加入したクライアントは配信データを視聴または聴視できる一方，データ配信サービスに加入していないクライアントは配信データを受信するものの，視聴および聴視できないようにする必要がある。

【０００４】

このためには，データの配信元が，クライアントのデータ配信サービスへの加入／非加入を正確に把握することが重要となり，また，加入したクライアントのみが配信データを視聴または聴視できるための暗号化技術が重要となる。

【０００５】

さらに，課金の方法としては，受信者が多数であることから，受信したデータ量に応じて課金を行える従量制課金が望ましいと考えられる。

【０００６】

【発明が解決しようとする課題】

しかし，現在インターネット上で実現されている暗号化技術は，データの送信者と受信者とが１対１（ユニキャスト）であることを前提としている。このため，多数の受信者を対象とするＩＰマルチキャストに関しては考慮がなされておらず，ＩＰマルチキャストでは，暗号化されていないデータが配信されてしまうのが現状である。

【０００７】

また，従来の従量制課金方式としては，ＣＳ放送等で採用されているペイパービュー（Pay per View）方式があるが，この方式は番組プログラム単位で課金を行うものである。したがって，番組プログラムの途中で視聴を中止したとしても番組全体を視聴した料金が課金される。このため，厳密には受信したデータ量で課金を行っているとは言えない。

【０００８】

インターネット上で画像や音楽を配信する場合には，プログラム単位よりも短い単位で受信者が加入／脱退することが考えられ，課金方式としても現状のペイパービュー方式よりもきめの細かい方式が要求される。

【０００９】

本発明は，このような背景に鑑みなされたものであり，その目的は，マルチキャスト通信において暗号化および復号化を適切に行えるようにすることにある。

【００１０】

また，本発明の目的は，マルチキャストグループに属するクライアントのうち，データ配信サービスに加入しているクライアントを把握可能とすることにある。

【００１１】

さらに，本発明の目的は，従量制課金を適切に行うことにある。

【００１２】

【課題を解決するための手段】

前記目的を達成するために，本発明の第１の側面によるマルチキャスト通信システムは，所定のデータ配信サービスに関するデータをマルチキャストにより送信するマルチキャストサーバと，マルチキャストグループに属し，前記データを受信する複数のクライアントとを有するマルチキャスト通信システムであって，前記マルチキャストサーバは，前記データを第１の暗号化鍵により暗号化するデータ暗号部と，前記データ暗号部により暗号化されたデータを，前記マルチキャストグループに属するクライアントにマルチキャストにより送信するデータ送信部と，前記第１の暗号化鍵を第２の暗号化鍵により暗号化する鍵暗号部と，前記鍵暗号部により暗号化された第１の暗号化鍵を，前記マルチキャストグループに属するクライアントのうち，前記データ配信サービスに加入したクライアントにユニキャストにより送信する鍵送信部と，を備え，前記複数のクライアントうち，前記データ配信サービスに加入したクライアントは，前記鍵送信部により送信される，暗号化された第１の暗号化鍵を受信する鍵受信部と，前記鍵受信部により受信された，暗号化された第１の暗号化鍵を復号化鍵により復号化する鍵復号部と，前記データ送信部により送信される，暗号化されたデータを，前記鍵復号部により得られた第１の暗号化鍵により復号するデータ復号部と，を備えている。

【００１３】

本発明の第１の側面によるマルチキャストデータ送信装置は，所定のデータ配

信サービスに関するデータを第１の暗号化鍵により暗号化するデータ暗号部と，前記データ暗号部により暗号化されたデータをマルチキャストにより，所定のマルチキャストグループに属するクライアントにマルチキャストにより送信するデータ送信部と，前記第１の暗号化鍵を第２の暗号化鍵により暗号化する鍵暗号部と，前記鍵暗号部により暗号化された第１の暗号化鍵を，前記マルチキャストに属するクライアントのうち，前記データ配信サービスに加入したクライアントにユニキャストにより送信する鍵送信部と，を備えている。

【００１４】

本発明の第１の側面によるマルチキャストデータ受信装置は，マルチキャストにより送信される，所定のデータ配信サービスに関するデータを受信するマルチキャストデータ受信装置であって，前記データ配信サービスに加入することにより得られる暗号化された第１の暗号化鍵を復号化する鍵復号部と，前記データ配信サービスに関するデータが前記第１の暗号化鍵により暗号化されたものを受信するデータ受信部と，前記データ受信部により受信された，暗号化されたデータを，前記鍵復号部の復号化により得られた第１の暗号化鍵により復号化するデータ復号部と，を備えている。

【００１５】

本発明の第１の側面によると，前記マルチキャストサーバ（またはマルチキャストデータ送信装置）は，前記データの暗号化に用いられる第１の暗号化鍵を第２の暗号化鍵により暗号化して，前記マルチキャストグループに属するクライアントのうち，前記データ配信サービスに加入したクライアント（またはマルチキャストデータ受信装置）にユニキャストにより送信する。前記データ配信サービスに加入したクライアントは，前記ユニキャストにより送信される，暗号化された第１の暗号化鍵を受信すると，これを復号化鍵により復号化する。続いて，前記マルチキャストサーバは，前記データを前記第１の暗号化鍵により暗号化して，前記マルチキャストグループに属するクライアントにマルチキャストにより送信する。前記クライアントは，前記暗号化されたデータを受信すると，これを前記復号化鍵の復号化により得られた前記第１の暗号化鍵により復号化する。

【００１６】

本発明の第１の側面によると，所定のデータ配信サービスに関するデータが暗号化される。また，該サービスに加入したクライアントのみが，暗号化されたデータを復号化できる一方，該サービスに加入していないクライアントに対してはデータの機密性が確保される。したがって，マルチキャスト通信において，データの暗号化を適切に行うことができる。

【００１７】

本発明の第２の側面によるマルチキャスト通信システムは，所定のデータ配信サービスに関するデータをマルチキャストにより送信するマルチキャストサーバと，マルチキャストグループに属し，前記データを受信する複数のクライアントとを有するマルチキャスト通信システムであって，前記マルチキャストサーバは，前記データを暗号化するためのデータ暗号化鍵を，所定の更新タイミングごとに，該更新タイミング前に有効なデータ暗号化鍵に，該更新タイミング前に有効なデータ暗号化鍵に対応する更新鍵を作用させることにより得られる関係にある，更新タイミング後に有効となるデータ暗号化鍵に更新する鍵更新部と，前記更新鍵を生成し，または，あらかじめ保持する更新鍵保持部と，前記データを現在有効なデータ暗号化鍵により暗号化するデータ暗号部と，前記データ暗号部により暗号化されたデータを，前記マルチキャストグループに属するクライアントにマルチキャストにより送信するデータ送信部と，前記更新タイミングごとに，更新タイミング後に有効なデータ暗号化鍵に対応する更新鍵を，該更新タイミング後に有効なデータ暗号化鍵により暗号化する鍵暗号部と，前記更新タイミングごとに，前記鍵暗号部により暗号化された更新鍵を前記クライアントにユニキャストまたはマルチキャストにより送信する更新鍵送信部と，を備え，前記複数のクライアントのうち，前記データ配信サービスに加入したクライアントは，前記データ送信部により送信される，暗号化されたデータを受信するデータ受信部と，前記データ受信部により受信される，前記暗号化されたデータを，前記現在有効なデータ暗号化鍵と同一の現在有効なデータ復号化鍵により復号化するデータ復号部と，前記更新鍵送信部により送信される，暗号化された更新鍵を受信する更新鍵受信部と，前記更新鍵受信部により受信される，暗号化された更新鍵を，前記現在有効なデータ復号化鍵により復号化する更新鍵復号部と，前記データ配信

サービスへの加入時には，外部から与えられ，その後は，前記更新タイミングごとに，該更新タイミング前に有効なデータ復号化鍵に，該更新タイミング前に有効なデータ復号化鍵による復号化により得られた前記更新鍵を作用させることにより，更新タイミング後に有効なデータ復号化鍵を生成し，前記更新タイミングごとに，前記更新タイミング前に有効なデータ復号化鍵を前記更新タイミング後に有効なデータ復号化鍵に更新するデータ復号化鍵更新部と，を備えている。

【００１８】

本発明の第２の側面によるマルチキャストデータ送信装置は，所定のデータ配信サービスに関するデータを暗号化するためのデータ暗号化鍵を，所定の更新タイミングごとに，該更新タイミング前に有効なデータ暗号化鍵に，該更新タイミング前に有効なデータ暗号化鍵に対応する更新鍵を作用させることにより得られる関係にある，更新タイミング後に有効となるデータ暗号化鍵に更新する鍵更新部と，前記更新鍵を生成し，または，あらかじめ保持する更新鍵保持部と，前記データを現在有効なデータ暗号化鍵により暗号化するデータ暗号部と，前記データ暗号部により暗号化されたデータを，所定のマルチキャストグループに属するクライアントにマルチキャストにより送信するデータ送信部と，前記更新タイミングごとに，更新タイミング後に有効なデータ暗号化鍵に対応する更新鍵を，該更新タイミング後に有効なデータ暗号化鍵により暗号化する鍵暗号部と，前記更新タイミングごとに，前記鍵暗号部により暗号化された更新鍵を前記クライアントにユニキャストまたはマルチキャストにより送信する更新鍵送信部と，を備えている。

【００１９】

本発明の第２の側面によると，前記マルチキャストサーバ（またはマルチキャストデータ送信装置）は，前記データを現在有効なデータ暗号化鍵により暗号化して，前記マルチキャストグループに属するクライアントにマルチキャストにより送信する。前記クライアントは，前記マルチキャストサーバから送信される，暗号化されたデータを受信して，前記暗号化されたデータを前記現在有効なデータ暗号化鍵と同一の現在有効な復号化鍵により復号化する。前記マルチキャストサーバは，前記データ暗号化鍵を，所定の更新タイミングごとに，該更新タイミ

ング前に有効なデータ暗号化鍵に，該更新タイミング前に有効なデータ暗号化鍵に対応する更新鍵を作用させることにより得られる関係にある，更新タイミング後に有効となるデータ暗号化鍵に更新する。前記マルチキャストサーバは，前記更新タイミングごとに，更新タイミング後に有効なデータ暗号化鍵に対応する更新鍵を，該更新タイミング後に有効なデータ暗号化鍵により暗号化して，前記クライアントにユニキャストまたはマルチキャストにより送信する。前記クライアントは，前記マルチキャストサーバから送信される，暗号化された更新鍵を受信して，該暗号化された更新鍵を，前記現在有効なデータ復号化鍵により復号化する。前記クライアントは，前記データ配信サービスへの加入時には，外部から与えられ，その後は，前記更新タイミングごとに，該更新タイミング前に有効なデータ復号化鍵に，該更新タイミング前に有効なデータ復号化鍵による復号化により得られた前記更新鍵を作用させることにより，更新タイミング後に有効なデータ復号化鍵を生成し，前記更新タイミングごとに，前記更新タイミング前に有効なデータ復号化鍵を前記更新タイミング後に有効なデータ復号化鍵に更新する。

【００２０】

本発明の第２の側面によっても，前述した第１の側面と同様の作用効果を得ることができる。

【００２１】

【発明の実施の形態】

以下に，本発明の実施の形態について図面を参照しながら説明するが，これらは例であって，本発明の技術的範囲を限定するものではない。

【００２２】

１．第１の実施の形態

図１は，本発明の第１の実施の形態によるマルチキャスト通信システムの全体構成を示すブロック図である。このマルチキャスト通信システムは，インターネット１に接続されたマルチキャストサーバ２と，複数のクライアント３ａ～３ｄを有するマルチキャストグループ３とを備えている。

【００２３】

マルチキャストサーバ（以下，単に「サーバ」という。）２は，データ配信サ

ービスを行うサーバであり，音楽，映像，テキスト等の配信データ（コンテンツ）を保持し，このコンテンツをインターネット１を介してＩＰマルチキャストによりマルチキャストグループ３に属するクライアント３ａ～３ｄに配信する。

【００２４】

クライアント３ａ～３ｄは，マルチキャストグループ３に属し，サーバ２からＩＰマルチキャストにより送信された配信データを受信する。図１では，クライアントの個数を，一例として４つにしているが，４つ以外の個数であってもよい。

【００２５】

このマルチキャスト通信システムでは，マルチキャストグループ３に属するクライアント３ａ～３ｄのうち，所定の加入手続（後述）を経てサーバ２のデータ配信サービスに加入したもの（加入者）だけが，このデータ配信サービスを受けることができるようになっている。これは，サーバ２が配信データを暗号化して送信するとともに，マルチキャストグループ３に属するクライアントが所定の加入手続を経てデータ配信サービスの加入者となり，暗号化された配信データを復号化するための復号鍵（共通鍵であり，以下「グループセッション鍵Ｋgr」という。）を入手することにより実現される。

【００２６】

すなわち，クライアント３ａ～３ｄは，マルチキャストグループ３に属するので，いずれのクライアントもサーバ２からのデータ配信サービスに関する配信データを受信するが，所定の加入手続を経て加入者とならなければ，受信した配信データを復号化して，その配信データを視聴，聴視等することができないようなっている。

【００２７】

また，このマルチキャスト通信システムでは，データ配信サービスの加入者に対して，従量制による課金がなされる。この従量制による課金は，本実施の形態では，データ配信サービスに加入してからの時間に従ってなされる。

【００２８】

以下，サーバ２，クライアント３ａ～３ｄ，およびこれらが行う処理の詳細に

ついて説明する。

【００２９】

図２は，サーバ２の構成を示すブロック図である。サーバ２は，制御部２０，データ暗号部２１，鍵暗号部２２，送受信部２３，コンテンツデータベース２４，および加入者リストデータベース２５を備えている。

【００３０】

制御部２０は，データ暗号部２１，鍵暗号部２２，送受信部２３，コンテンツデータベース２４，および加入者リストデータベース２５を制御するとともに，後に詳述する加入者の加入および脱退の処理，加入に伴うグループセッション鍵Ｋgrの配布，従量制による課金等の処理を行う。また，制御部２０は，グループセッション鍵Ｋgrを保持し，データ暗号部２１および鍵暗号部２２に暗号化処理を実行させる際に，これらデータ暗号部２１および鍵暗号部２２にグループセッション鍵Ｋgrを与える。

【００３１】

コンテンツデータベース２４は，ハードディスク，半導体メモリ等の記憶装置，または，ＤＶＤ，ＣＤ等の記録媒体およびその読み取り装置により構成され，マルチキャストグループ３に送信される配信データ（コンテンツ）を記憶する。このコンテンツデータベース２４は，制御部２０の制御の下，配信データをデータ暗号部２１に与える。

【００３２】

データ暗号部２１は，グループセッション鍵（共通鍵）Ｋgrを制御部２０から受け取り，制御部２０の制御の下，コンテンツデータベース２４からの配信データをグループセッション鍵Ｋgrにより暗号化して送受信部２３に与える。暗号化の方法としては，ＤＥＳ（Data Encryption Standard）等が用いられる。なお，グループセッション鍵Ｋgrは，データ暗号部２１が保持していてもよい。

【００３３】

加入者リストデータベース２５は，ハードディスク，半導体メモリ等の記憶装置，または，ＤＶＤ，ＣＤ等の記録媒体およびその読み取り／書き込み装置により構成され，図３に示す加入者リストを記憶する。加入者リストは，マルチキャ

ストグループ３に属するクライアント３ａ～３ｄのうち，所定の加入手続を経て，サーバ２のデータ配信サービスに加入したクライアントのリストである。この加入者リストに登録された加入者は，グループセッション鍵Ｋgrをサーバ２から提供され，これにより，サーバ２からの暗号化された配信データを復号化することができる。

【００３４】

図３に示すように，加入者リストを構成する各リストセルは，加入者名，鍵復号鍵Ｋｍ，および加入日時を有する。

【００３５】

「加入者名」は，あるクライアントを他のクライアントからユニークに識別するための名称，識別子等であり，この加入者名としては，たとえば，データ配信サービスの提供者が加入者に与えるユニークなユーザＩＤ，そのクライアントのＩＰアドレス等が使用される。

【００３６】

「鍵復号鍵」は，グループセッション鍵Ｋgrを暗号化し，かつ，暗号化されたグループセッション鍵Ｋgr（以下「暗号化グループセッション鍵Ｋgrｘ」という。）を復号化するための共通鍵である。この鍵復号鍵は，加入者も所有する。各加入者に対してそれぞれ個別の鍵復号鍵Ｋｍ(Ａ)，Ｋｍ(Ｂ)等が設けられることが好ましい。

【００３７】

「加入日時」は，加入者がデータ配信サービスに加入した日時である。本実施の形態では，この加入日時から脱退日時までの時間に基づいて，各加入者から徴収する料金（データ配信サービス料）が計算される。

【００３８】

マルチキャストグループ３に属するクライアントがデータ配信サービスに新たに加入すると，制御部２０は，新たなリストセルを生成し，生成したリストセルを加入者リストに追加する。一方，既に加入者となっているクライアントがデータ配信サービスから脱退すると，制御部２０は，脱退した加入者のリストセルを加入者リストから消去（削除）する。

【００３９】

鍵暗号部２２は，制御部２０からグループセッション鍵Ｋgrを受け取り，制御部２０の制御の下，送信先のクライアントの鍵復号鍵Ｋｍを加入者リストから読み出し，読み出した鍵復号鍵Ｋｍによりグループセッション鍵Ｋgrを暗号化する。暗号化の方法としては，ＤＥＳ（Data Encryption Standard）等が用いられる。そして，鍵暗号部２２は，暗号化により得られた暗号化グループセッション鍵Ｋgrｘを送受信部２３に与える。たとえば，クライアント３ａにグループセッション鍵Ｋgrを送信する場合に，鍵暗号部２２は，グループセッション鍵Ｋgrをクライアント３ａの鍵復号鍵Ｋｍ(Ａ)を用いて暗号化する。

【００４０】

送受信部２３は，インターネット１とのインタフェース装置である。この送受信部２３は，制御部２０の制御の下，データ暗号部２１からのデータをマルチキャストグループ３に属するクライアントにインターネット１を介してＩＰマルチキャストにより送信するとともに，鍵暗号部２２からの暗号化グループセッション鍵Ｋgrｘをインターネット１を介してユニキャストによりクライアントに送信する。また，送受信部２３は，マルチキャストグループ３に属するクライアントからインターネット１を介して送信されてきたデータを受信し，制御部２０に与える。

【００４１】

クライアント３ａ～３ｄには，サーバ２からの配信データを受信するためのハードウェア装置として，配信データ受信装置（またはアダプタ）が取り付けられる。この配信データ受信装置は，たとえば市販されることにより，いずれのユーザも購入可能な状況に置かれ，クライアント３ａ～３ｄのユーザがデータ配信サービスに加入するために購入するものである。この配信データ受信装置には，暗号化グループセッション鍵Ｋgrｘを復号化するための鍵復号鍵Ｋｍがあらかじめ記憶されている。

【００４２】

図４は，配信データ受信装置（またはアダプタ）３００の構成を示すブロック図である。この配信データ受信装置３００は，制御部３０，送受信部３１，デー

タ復号部３２，鍵復号部３３，および鍵復号鍵保持部３４を備えている。

【００４３】

制御部３０は，送受信部３１，データ復号部３２，鍵復号部３３，および鍵復号鍵保持部３４を制御するとともに，後に詳述する加入者の加入および脱退の処理，脱退に伴うグループセッション鍵Ｋgrの消去（または削除，破壊），鍵復号鍵Ｋｍの消去（または削除，破壊）等の処理を行う。

【００４４】

送受信部３１は，インターネット１とのインタフェース装置であり，制御部３０の制御の下，制御部３０から与えられる受信要求（後述）をインターネット１を介してサーバ２に送信する。また，送受信部３１は，制御部３０の制御の下，サーバ２からインターネット１を介して送信されてきた暗号化グループセッション鍵Ｋgrｘおよび暗号化された配信データ（以下「暗号化配信データ」という。）を受信し，それぞれ鍵復号部３３およびデータ復号部３２に与える。

【００４５】

鍵復号鍵保持部３４は，鍵復号鍵Ｋｍを保持する。第三者が鍵復号鍵Ｋｍを容易に読み出すことができないようにするために，鍵復号鍵Ｋｍは，ハードウェア回路（たとえばＩＣチップ）として鍵復号鍵保持部３４に記憶（形成）されていることが好ましい。また，鍵復号鍵Ｋｍは，配信データ受信装置ごと（すなわちクライアントごと）に異なるものが記憶されていることが好ましい。

【００４６】

鍵復号部３３は，サーバ２から送信された暗号化グループセッション鍵Ｋgrｘを鍵復号鍵Ｋｍによりに復号化し，復号化により得られたグループセッション鍵Ｋgrを保持する。なお，データ復号部３２がグループセッション鍵Ｋgrを保持してもよい。

【００４７】

データ復号部３２は，サーバ２から送信された暗号化配信データを，鍵復号部３３が保持するグループセッション鍵Ｋgrを用いて復号化し，復号化により得られた配信データを，配信データ受信装置３００が取り付けられたクライアントに与える。クライアントは，その表示装置（ＣＲＴディスプレイ，液晶ディスプレ

イ等），スピーカ等に，配信データを出力する。これにより，クライアントのユーザは，配信データを視聴，聴視等することができる。なお，配信データは，出力される前にクライアントのハードディスク等の記憶装置（図示略）に記憶されてもよい。

【００４８】

後述するように，鍵復号鍵保持部３４に記憶された鍵復号鍵Ｋｍ，および，鍵復号部３３が保持するグループセッション鍵Ｋgrは，クライアントがデータ配信サービスから脱退することによって，制御部３０により消去（または削除，破壊）される。

【００４９】

図５は，サーバ２およびマルチキャストグループ３に属するクライアント（ここでは，クライアント３ｃとする。）の処理の流れを示すシーケンス図である。このシーケンス図に示す処理は，サーバ２のデータ配信サービスに未加入のクライアント３ｃが，データ配信サービスに加入する場合を説明している。

【００５０】

まず，クライアント３ｃは，データ配信サービスに加入していないので，サーバ２が送信した暗号化配信データを受信できるものの，これを復号化できない状態にある。

【００５１】

この状態において，クライアント３ｃのユーザは，まず，配信データ受信装置３００を購入し，これをクライアント３ｃに取り付ける。クライアント３ｃに取り付けられた配信データ受信装置３００には，鍵復号鍵Ｋｍ(Ｃ)が記憶されているものとする。

【００５２】

配信データ受信装置３００をクライアント３ｃに取り付けることにより，制御部３０は，データ配信サービスの加入手続として，受信要求を送受信部３１およびインターネット１を介してサーバ２に送信する（ステップＳ１）。この受信要求には，クライアント３ｃのクライアント名と，クライアント３ｃに取り付けられた配信データ受信装置３００を他の配信データ受信装置からユニークに識別す

るための機器番号（識別番号，シリアル番号）とが含まれている。

【００５３】

この機器番号は，制御部３０にあらかじめ記憶されているものが制御部３０により送信されてもよいし，配信データ受信装置３００の基板等に貼付されているものが，クライアント３ｃのユーザによってクライアント３ｃから入力され，制御部３０によって送信されてもよい。また，この機器番号は，配信データ受信装置３の購入後，直ちに販売店からサーバ２に通知され，制御部２０に記憶される。

【００５４】

クライアント３ｃからインターネット１を介して送信された受信要求は，サーバ２の送受信部２３（図２参照）を介して制御部２０に与えられる。制御部２０は，受信要求に含まれる機器番号が，販売店から通知されたものであるかどうかを確認し，受信を許可するかどうかを判断する（ステップＳ２１）。

【００５５】

制御部２０は，受信要求に含まれる機器番号が販売店から通知されたものである場合には受信を許可し（ステップＳ２１でＹＥＳ），そうでない場合には受信を許可しない（ステップＳ２１でＮＯ）。

【００５６】

受信を許可しない場合に，制御部２０は，受信要求を無視する（ステップＳ３３）。これにより，クライアント３ｃは，配信データを視聴または聴視することができない状態が続くこととなる。

【００５７】

受信を許可する場合に，制御部２０は，加入者リストのリストセルを生成し，生成したリストセルを加入者リストデータベース２５の加入者リストに追加する（ステップＳ２３）。このリストセルのクライアント名の欄には，受信要求に含まれるクライアント名が格納され，鍵復号鍵の欄には，配信データ受信装置３００の鍵復号鍵保持部３４に記憶された鍵復号鍵（「Ｋｍ(Ｃ)」とする。）が格納される。また，加入日時として，受信要求の受信日時（またはリストセル生成日時，データベース２５への登録日時等）が格納される。

【００５８】

鍵復号鍵Ｋｍが配信データ受信装置３００ごとに異なる場合には，配信データ受信装置３００の機器番号と，その鍵復号鍵保持部３４に記憶された鍵復号鍵Ｋｍとを対応させた機器番号／鍵復号鍵対応データがサーバ２（たとえば制御部２０または図示しない記憶部）にあらかじめ記憶される。これにより，制御部２０は，機器番号に対応する鍵復号鍵Ｋｍをリストセルの鍵復号鍵に格納する。

【００５９】

続いて，鍵暗号部２２は，グループセッション鍵Ｋgrを鍵復号鍵Ｋｍ(Ｃ)により暗号化グループセッション鍵Ｋgrｘに暗号化し，暗号化グループセッション鍵Ｋgrｘを送受信部２３を介してユニキャストによりクライアント３ｃに送信する（ステップＳ２５）。

【００６０】

配信データ受信装置３００の送受信部３１は，暗号化グループセッション鍵Ｋgrｘを受信すると，受信した暗号化グループセッション鍵Ｋgrｘを鍵復号部３３に与える。鍵復号部３３は，鍵復号鍵保持部３４が保持する鍵復号鍵Ｋｍ(Ｃ)により暗号化グループセッション鍵Ｋgrｘを復号化し，復号化されたグループセッション鍵Ｋgrを保持する（ステップＳ５）。これにより，加入手続は完了する。

【００６１】

その後，サーバ２のデータ暗号部２１は，コンテンツデータベース２４に記憶された配信データをグループセッション鍵Ｋgrにより暗号化し，送受信部２３を介してＩＰマルチキャストによりマルチキャストグループ３に送信する（ステップＳ２７）。

【００６２】

クライアント３ｃの送受信部３１は，暗号化配信データを受信すると，この暗号化配信データを，データ復号部３２に与える。データ復号部３２は，鍵復号部３３が保持するグループセッション鍵Ｋgrにより暗号化配信データを復号化し，復号化した配信データをクライアント３ｃに与える。クライアント３ｃは，配信データに映像データが含まれる場合には，該映像データを表示装置に表示し，音声データが含まれる場合には，該音声をスピーカから出力する（ステップＳ７）

【００６３】

このようなステップＳ５およびＳ７の処理が，クライアント３ｃがデータ配信サービスから脱退するまで繰り返される（ステップＳ９でＮＯ）。

【００６４】

一方，クライアント３ｃがデータ配信サービスから脱退する場合には（ステップＳ９でＹＥＳ），クライアント３ｃから脱退要求が制御部３０に与えられる。この脱退要求は，たとえば，クライアント３ｃのユーザがクライアント３ｃの入力装置（キーボード等）を介して入力したものである。

【００６５】

制御部３０は，クライアント３ｃから脱退要求を受信すると，鍵復号鍵保持部３４に保持された鍵復号鍵Ｋｍ(Ｃ)を消去（または削除，破壊）するとともに，鍵復号部３３に保持されたグループセッション鍵Ｋgrを消去（または削除，破壊）する。そして，制御部３０は，この消去に伴い，消去したことを示すデータとして消去値を生成する（ステップＳ１１）。

【００６６】

この消去値としては，たとえば，配信データ受信装置３００の機器番号やクライアントのＩＰアドレス等に所定の演算（所定の方程式による演算，ハッシュ演算等）を施したものを使用することができる。また，配信データがストリームデータであり，ストリーミングごとに番号が付加されている場合には，このインデックス番号に所定の演算を施したものを消去値として使用することもできる。さらに，脱退要求送信時（配信データの受信終了時）の日時に所定の演算を施したものを消去値として使用することもできる。所定の演算は，配信データ受信装置３００のハードウェア回路（たとえばＩＣチップ）により実行され，どのような演算が実行されているかを第三者が容易に知ることができないようになっている。

【００６７】

制御部３０は，生成した消去値をクライアント名とともに，送受信部３１を介してサーバ２に送信する（ステップＳ１１）。

【００６８】

配信データ受信装置３００において，鍵復号鍵Ｋｍ(Ｃ)およびグループセッション鍵Ｋgrが消去されることにより，その後，クライアント３ｃは，暗号化配信データを受信するが，これを復号化できなくなる。その結果，クライアント３ｃのユーザは配信データを視聴，聴視等できなくなる。

【００６９】

サーバ２の制御部２０は，消去値が正しいかどうかを判断する（ステップＳ２９）。この判断は，制御部２０が制御部３０と同じ演算を行い，その演算結果と受信した消去値とを比較することにより行われる。たとえば，消去値として，機器番号に所定の演算を施したものが使用される場合には，制御部２０も，制御部３０と同じ演算を，消去値を送信した配信データ受信装置３００（クライアント３ｃ）の機器番号に対して実行し，その演算結果と消去値とを比較することにより，消去値が正しいかどうかが判断される。

【００７０】

また，インデックス番号に所定の演算を施したもの，または，受信終了日時に所定の演算を施したものが消去値として使用される場合には，消去値に逆演算を施し，逆演算結果が妥当なものかどうかにより，判断が行われる。この場合には，逆演算結果（インデックス番号または受信終了日時）から，クライアント３ｃがストリームデータをどこまで受信したか，または，受信終了日時が判明するので，これらに基づいて従量制課金を行うこともできる。

【００７１】

消去値が正しい場合には（ステップＳ２９でＹＥＳ），制御部２０は，クライアント３ｃのリストセルの加入日時と消去値を受信した日時とから，サービスに加入していた時間を求め，この時間に基づいて従量制のサービス料金を算出する。このサービス料金は，クライアント３ｃのユーザに課金され，徴収されることとなる。なお，課金および徴収は，加入期間中，一定期間（たとえば１箇月）ごとに行い，脱退時は，脱退直前に課金した時点から脱退時までの期間分の課金を行うこともできる。また，消去値からインデックス値または受信終了日時が得られる場合には，このインデックス値または受信終了日時に基づいて従量制の課金

を行うこともできる。

【００７２】

その後，制御部２０は，クライアント３ｃのリストセルを加入者リストデータベース２５の加入者リストから消去する。消去により，その後，クライアント３ｃには，サービスの課金は行われなくなる。

【００７３】

一方，消去値が正しくない場合には（ステップＳ２９でＮＯ），制御部２０は，クライアント３ｃを違反者として，クライアント３ｃに警告を送信する（ステップＳ３５）。

【００７４】

このように，本実施の形態では，ＩＰマルチキャスト通信において，配信データが暗号化されるとともに，データ配信サービスに正規に加入した者のみが復号化鍵を入手する。したがって，ＩＰマルチキャストにおいて，暗号化が適切に行われ，その結果，データ配信サービスに正規に加入した者のみが配信データを視聴，聴視等することができ，それ以外の者に対してはデータの機密性が確保される。また，本実施の形態では，配信データの提供元であるサーバ２において，データ配信サービスの加入者を管理／把握することができる。さらに，本実施の形態によると，ペイパービュー方式による課金よりも木目の細かい従量制の課金を行うことができる。

【００７５】

なお，サーバ２は，各クライアント（各配信データ受信装置３００）の鍵復号鍵Ｋｍを，前述したように機器番号／鍵復号鍵対応データから得るのではなく，配信データ受信装置３００が自己の鍵復号鍵Ｋｍをサーバ２の公開鍵Ｋｐにより暗号化してサーバ２に送信し，この送信された鍵をサーバ２が秘密鍵Ｋｓを用いて復号化することにより得ることもできる。この場合に，サーバ２の機器番号／鍵復号鍵対応データは特に設ける必要はなくなる。この公開鍵および秘密鍵を用いる公開鍵暗号方式としては，ＲＳＡ（Rivest Shamir Adleman），楕円曲線暗号等を使用することができる。

【００７６】

また，公開鍵基盤（ＰＫＩ：Public Key Infrastructure）を利用することもできる。すなわち，各クライアントは，データ配信サービスに加入する際に，ＰＫＩの認証局からディジタル証明書（公開鍵および秘密鍵のセット）の発行を受ける。そして，サーバ２は，クライアントからの受信要求を受けると，このディジタル証明書の公開鍵（クライアントの公開鍵）を取得し，この公開鍵を用いてグループセッション鍵Ｋgrを暗号化し，受信要求を送信したクライアントは，暗号化により得られた暗号化グループセッション鍵Ｋgrｘをディジタル証明書の秘密鍵により復号化して，グループセッション鍵Ｋgrを取得することができる。

【００７７】

２．第２の実施の形態

グループセッション鍵Ｋgrを定期的に更新することにより，配信データの機密性を確保することもできる。

【００７８】

図６は，本発明の第２の実施の形態によるマルチキャスト通信システムの全体構成を示すブロック図である。このマルチキャスト通信システムは，インターネット１に接続されたマルチキャストサーバ４と，複数のクライアント５ａ～５ｄを有するマルチキャストグループ５とを備えている。このマルチキャスト通信システムの全体構成は，図１に示す第１の実施の形態のものと同じであるので，このマルチキャスト通信システムの全体構成の説明はここでは省略する。

【００７９】

図７は，第２の実施の形態によるサーバ４の構成を示すブロック図である。サーバ４は，制御部４０，データ暗号部４１，鍵暗号部４２，送受信部４３，コンテンツデータベース４４，加入者リストデータベース４５，および鍵データベース４６を備えている。

【００８０】

制御部４０は，データ暗号部４１，鍵暗号部４２，送受信部４３，コンテンツデータベース４４，鍵データベース４５，および加入者リストデータベース４６を制御するとともに，後に詳述する加入者の加入および脱退の処理，加入に伴うグループセッション鍵Ｋgrの配布，従量制による課金等の処理を行う。また，制

御部４０は，グループセッション鍵Ｋgrを一定時間Ｔ１ごとに更新する。

【００８１】

コンテンツデータベース４４は，第１の実施の形態におけるコンテンツデータベース２４（図２参照）と同様のものである。このコンテンツデータベース４４に記憶された配信データは，制御部４０の制御の下，読み出され，データ暗号部４１に与えられる。

【００８２】

データ暗号部４１は，グループセッション鍵（共通鍵）Ｋgrを制御部４０から受け取り，制御部４０の制御の下，コンテンツデータベース４４からの配信データをグループセッション鍵Ｋgrにより暗号化して送受信部４３に与える。暗号化の方法としては，ＤＥＳ等が用いられる。なお，グループセッション鍵Ｋgrは，データ暗号部４１が保持していてもよい。

【００８３】

加入者リストデータベース４６は，第１の実施の形態における加入者リストデータベース２５（図２参照）と同様に構成され，所定の加入手続を経てデータ配信サービスに加入した加入者のリストを記憶する。この加入者リストは，図３に示す第１の実施の形態のものとほぼ同じであるが，本実施の形態では，第１の実施の形態における鍵復号鍵Ｋｍの欄は設けられない。

【００８４】

鍵データベース４５は，図８に示すように，複数のグループセッション鍵Ｋgrと，各グループセッション鍵Ｋgrに対応する鍵更新鍵Ｋｕとが対応した鍵データを保持する。

【００８５】

符号ｉを任意の正の整数とすると，グループセッション鍵Ｋgr(ｉ＋１)は，グループセッション鍵Ｋgr(ｉ)に，これに対応する鍵更新鍵Ｋｕ(ｉ)を作用させることにより得られる。この作用として，たとえばグループセッション鍵Ｋgr(ｉ)と鍵更新鍵Ｋｕ(ｉ)とを所定の方程式に代入して演算する処理（グループセッション鍵Ｋgr(ｉ)を鍵更新鍵Ｋｕ(ｉ)により暗号化する処理を含む。）がある。グループセッション鍵Ｋgr(１)は，グループセッション鍵の初期値として，鍵デー

タベース４５にあらかじめ与えられる。

【００８６】

これら複数のグループセッション鍵Ｋgr群は，任意のグループセッション鍵Ｋgr(ｉ)で暗号化されたデータが同一のグループセッション鍵Ｋgr(ｉ)でのみ復号化でき，他のグループセッション鍵Ｋgr(ｊ)（ｉ≠ｊ）では復号化できないように構成されている。

【００８７】

制御部４０は，グループセッション鍵Ｋgrを一定時間Ｔ１ごとにKgr(ｉ)からKgr(ｉ＋１)に更新して行く。そして，制御部４０は，この更新時（更新タイミング）に，鍵更新鍵Ｋｕ(ｉ)をグループセッション鍵Ｋgr(ｉ)により暗号化し，暗号化した鍵更新鍵をマルチキャストグループ５に属するクライアントに送信する。

【００８８】

なお，鍵更新鍵Ku(ｉ)は，次々と新しいものが制御部４０により生成されてもよいし，所定の個数ｎだけがあらかじめ用意されていてもよい。前者の場合には，たとえば擬似乱数発生器により発生された擬似乱数等を，新たな鍵更新鍵として使用することができる。後者の場合には，第ｎ番目のグループセッション鍵Kgr(ｎ)に鍵更新鍵Ｋｕ(ｎ)を作用させると，第１番目のグループセッション鍵Kgr(１)が生成されるようなサイクリックな構成とされる。

【００８９】

また，鍵データベース４５には，必ずしも複数のグループセッション鍵が記憶されている必要はなく，現在有効なグループセッション鍵Ｋgr（すなわち現在，配信データの暗号化に使用されているグループセッション鍵Ｋgr）のみが記憶されていてもよい。この場合に，制御部４０は，鍵更新時に，現在有効なグループセッション鍵Kgr(ｉ)に，これに対応する鍵更新鍵Ｋｕ(ｉ)を作用させることにより，次のグループセッション鍵Kgr(ｉ＋１)を作成して行くこととなる。

【００９０】

鍵暗号部４２は，制御部４０からグループセッション鍵Ｋgr(ｉ)を受け取る。そして，鍵暗号部４２は，制御部４０のグループセッション鍵の更新時に，グル

ープセッション鍵Ｋgr(ｉ)に対応する鍵更新鍵Ｋｕ(ｉ)を鍵データベース４５から読み出してグループセッション鍵Ｋgr(ｉ)により暗号化し，暗号化された鍵更新鍵Ｋｕ(ｉ)（以下「暗号化鍵更新鍵Ｋｕｘ(ｉ)」という。）を送受信部４３に与える。この暗号化鍵更新鍵Ｋｕｘ(ｉ)は，送受信部４３からインターネット１を介してマルチキャストグループ５に属するクライアントに送信される。暗号化の方法としては，ＤＥＳ等が用いられる。

【００９１】

送受信部４３は，インターネット１とのインタフェース装置であり，制御部２０の制御の下，データ暗号部４１または鍵暗号部４２からのデータをインターネット１を介してマルチキャストグループ５に属するクライアントに送信するとともに，マルチキャストグループ５に属するクライアントからインターネット１を介して送信されてきたデータを受信し，制御部４０に与える。

【００９２】

図９は，第２の実施の形態によるクライアント５ａ～５ｄのそれぞれの構成を示すブロック図である。クライアント５ａ～５ｄはいずれも同じ構成を有するので，以下では，クライアント５ｃを代表として説明することとする。

【００９３】

クライアント５ｃは，制御部５０，送受信部５１，データ復号部５２，鍵復号部５３，出力部５４，入力部５５，および鍵生成部５６を備えている。

【００９４】

制御部５０は，送受信部５１，データ復号部５２，鍵復号部５３，出力部５４，および入力部５５を制御するとともに，後に詳述する加入者の加入および脱退の処理，脱退に伴うグループセッション鍵Ｋgr(ｉ)の消去（削除，破壊）等の処理を行う。

【００９５】

送受信部５１は，インターネット１とのインタフェース装置であり，制御部５０の制御の下，制御部５０から与えられる受信要求（後述）をインターネット１を介してサーバ４に送信する。また，送受信部５１は，制御部５０の制御の下，サーバ４からインターネット１を介して送信されてきた暗号化配信データおよび

暗号化鍵更新鍵Ｋｕｘ(ｉ)を受信し，それぞれデータ復号部５２および鍵復号部５３に与える。

【００９６】

鍵復号部５３は，サーバ４から送信される暗号化鍵更新鍵Ｋｕｘ(ｉ)をグループセッション鍵Ｋgr(ｉ)で復号化し，復号化により得られた鍵更新鍵Ｋｕ(ｉ)を保持する。なお，復号化により得られた鍵更新鍵Ｋｕ(ｉ)は，鍵生成部５６に与えられ，保持されてもよい。

【００９７】

鍵生成部５６は，鍵復号部５３が保持する鍵更新鍵Ｋｕ(ｉ)を受け取り，この鍵更新鍵Ｋｕ(ｉ)と，これに対応するグループセッション鍵Ｋgr(ｉ)とから，次のグループセッション鍵Ｋgr(ｉ＋１)を生成する。そして，鍵生成部５６は，現在有効なグループセッション鍵Ｋgr(ｉ)および次に有効となるグループセッション鍵Ｋgr(ｉ＋１)を保持する。

【００９８】

データ復号部５２は，サーバ４から送信される暗号化配信データを，鍵生成部５６が保持する現在有効なグループセッション鍵Ｋgr(ｉ)を用いて復号化し，復号化した配信データを出力部５４に与える。

【００９９】

出力部５４は，表示装置（ＣＲＴディスプレイ，液晶ディスプレイ等）および／またはスピーカ等により構成され，データ復号部５２から与えられた配信データを出力する。これにより，クライアント５ｃのユーザは，配信データを視聴，聴視等することができる。なお，配信データは，出力部５４により出力される前にクライアント５ｃのハードディスク等の記憶装置（図示略）に記憶されてもよい。

【０１００】

後述するように，鍵生成部５６に記憶されたグループセッション鍵Ｋgr(ｉ)およびＫgr(ｉ＋１)は，クライアント５ｃがデータ配信サービスから脱退することによって，制御部５０により消去（または削除，破壊）される。

【０１０１】

図１０は，サーバ４およびマルチキャストグループ５に属するクライアント（ここでは，クライアント５ｃとする。）の処理の流れを示すシーケンス図である。このシーケンス図に示す処理は，サーバ４のデータ配信サービスに未加入のクライアント５ｃが，データ配信サービスに加入する場合を説明している。

【０１０２】

まず，クライアント５ｃの制御部５０は，クライアント５ｃの入力部５５を介して与えられるユーザの指示に従って，データ配信サービスの加入手続を行う。この加入手続は，制御部５０が受信要求を送受信部５１およびインターネット１を介してサーバ４に送信することにより行われる（ステップＳ５１）。この受信要求には，クライアント５ｃのクライアント名が含まれる。

【０１０３】

受信要求は，サーバ４の送受信部４３を介して制御部４０に与えられる。制御部４０は，受信要求に含まれるクライアント名が，マルチキャストグループ５に属するクライアントのもので，かつ，データ配信サービスに加入していないものであるかどうかを確認し，受信を許可するかどうかを判断する（ステップＳ８１）。

【０１０４】

制御部４０は，受信要求に含まれるクライアント名がマルチキャストグループ５に属するクライアントのもので，かつ，データ配信サービスに加入していないものである場合には受信を許可し（ステップＳ８１でＹＥＳ），そうでない場合には受信を許可しない（ステップＳ８１でＮＯ）。

【０１０５】

受信を許可しない場合に，制御部４０は，受信要求を無視する（ステップＳ８５）。これにより，クライアント５ｃは，配信データを視聴または聴視することができない状態が続くこととなる。

【０１０６】

受信を許可する場合に，制御部４０は，クライアント５ｃのための加入者リストのリストセルを生成し，生成したリストセルを加入者リストデータベース４６の加入者リストに追加する（ステップＳ８３）。このリストセルのクライアント

名の欄には，受信要求に含まれるクライアント名が格納され，加入日時の欄には，受信要求の受信日時（またはリストセル生成日時，データベース４６への登録日時等）が格納される。

【０１０７】

続いて，制御部４０（または鍵暗号部４２）は，受信要求の受信時において有効なグループセッション鍵（Ｋgr(ｉ)とする。）を暗号化し，送受信部４３を介してクライアント５ｃにユニキャストにより送信する（ステップＳ８７）。この暗号化の方法としては，たとえば，サーバ４が共通鍵Ｋｃでグループセッション鍵Kgr(ｉ)を暗号化するとともに，この共通鍵Ｋｃをクライアント５ｃの公開鍵Ｋｐにより暗号化してクライアント５ｃに送信する方法がある。クライアント５ｃは秘密鍵Ｋｓにより，暗号化された共通鍵Ｋｃを復号化し，さらに暗号化グループセッション鍵Kgrx(ｉ)を共通鍵Ｋｃにより復号し，グループセッション鍵Kgr(ｉ)を得る（ステップＳ５３）。

【０１０８】

続いて，鍵暗号部４２は，グループセッション鍵Kgr(ｉ)により鍵更新鍵Ｋｕ(ｉ)を暗号化して暗号化鍵更新鍵Ｋｕｘ(ｉ)を生成し，この暗号化鍵更新鍵Ｋｕｘ(ｉ)をクライアント５ｃにユニキャストにより送信する（ステップＳ８９）。

【０１０９】

続いて，データ暗号部４１は，コンテンツデータベース４４に記憶された配信データをグループセッション鍵Kgr(ｉ)により暗号化し，暗号化配信データをマルチキャストグループ５にマルチキャスト送信する（ステップＳ９１）。なお，暗号化鍵更新鍵Ｋｕｘ(ｉ)のユニキャストによる送信時（ステップＳ８９）が他のクライアント（群）の鍵更新時（更新タイミング）に該当する場合には，この暗号化鍵更新鍵Ｋｕｘ(ｉ)は，ユニキャストによりクライアント５ｃにのみ送信されるのではなく，マルチキャストグループ５にマルチキャストにより送信されてもよい。

【０１１０】

クライアント５ｃの鍵復号部５３は，暗号化鍵更新鍵Ｋｕｘ(ｉ)をグループセッション鍵Kgr(ｉ)により復号化し，復号化された鍵更新鍵Ｋｕ(ｉ)を保持する

(ステップＳ５５)。続いて，鍵生成部５６は，グループセッション鍵Ｋgr(ｉ)に，鍵復号部５３に保持された鍵復号鍵Ｋｕ(ｉ)を作用させて，次のグループセッション鍵Ｋgr(ｉ＋１)を生成し，保持する（ステップＳ５７）。

【０１１１】

一方，データ復号部５２は，暗号化配信データを，グループセッション鍵Ｋgr(ｉ)により復号化し，復号化により得られた配信データを出力部５４に与える（ステップＳ５９）。出力部５４は配信データを出力し，これにより，クライアント５ｃのユーザは配信データを視聴，聴視等することができる（ステップＳ６１）。

【０１１２】

サーバ４において時間Ｔ１ごとの鍵更新タイミングが到来するまで，配信データは，このグループセッション鍵Ｋgr(ｉ)により暗号化され，送信される（ステップＳ９３でＮＯ，Ｓ９１）。

【０１１３】

鍵更新タイミングが到来すると（ステップＳ９３でＹＥＳ），制御部４０は，グループセッション鍵Ｋgr(ｉ)を次のグループセッション鍵Ｋgr(ｉ＋１)に更新する（ステップＳ９５）。

【０１１４】

続いて，鍵暗号部４２は，グループセッション鍵Ｋgr(ｉ＋１)に対応する鍵更新鍵Ｋｕ(ｉ＋１)をグループセッション鍵Ｋgr(ｉ＋１)により暗号化し，暗号化により得られた暗号化鍵更新鍵Ｋｕｘ(ｉ＋１)をマルチキャストグループ５にマルチキャスト送信する（ステップＳ９７）。

【０１１５】

クライアント５ｃの送受信部５１がこの暗号化鍵更新鍵Ｋｕｘ(ｉ＋１)を受信すると，制御部５０は，鍵生成部５６に，グループセッション鍵Ｋgr(ｉ)を次のグループセッション鍵Ｋgr(ｉ＋１)に更新するように指示する。以後，データ復号部５２は，グループセッション鍵Ｋgr(ｉ＋１)により暗号化配信データを復号化する。直前に使用されていたグループセッション鍵Ｋgr(ｉ)および鍵更新鍵Ｋｕ(ｉ)は，制御部５０により消去（または削除，破壊）される。

【０１１６】

また，これと同時に，鍵復号部５３は，暗号化鍵更新鍵Ｋｕｘ(ｉ＋１)をグループセッション鍵Ｋgr(ｉ＋１)により復号化する。鍵生成部５６は，グループセッション鍵Ｋgr(ｉ＋１)に，復号化により得られた鍵更新鍵Ｋｕ(ｉ＋１)を作用させ，次のグループセッション鍵Ｋgr(ｉ＋２)を生成し，保持する。

【０１１７】

マルチキャストグループ５に属し，かつ，データ配信サービスに加入している他のクライアントも同様の処理を行う。

【０１１８】

このようなグループセッション鍵の更新が時間Ｔ１ごとに繰り返される。これにより，データ配信サービスに加入していない第三者が，配信データを復号化して視聴，聴視等することが困難となり，配信データの高い機密性が確保される。

【０１１９】

一方，クライアント５ｃがデータ配信サービスから脱退する場合には，前述した第１の実施の形態と同様に，制御部５０は，鍵生成部５６に記憶された現在有効なグループセッション鍵および次のグループセッション鍵，ならびに鍵更新鍵をすべて消去（削除，破壊）する（図１０に図示せず）。これにより，クライアント５ｃは，以後，暗号化配信データを復号化することができず，また，以後のグループセッション鍵の更新も行うことができない。その結果，脱退後，クライアント５ｃのユーザは，配信データを視聴，聴視等できなくなる。

【０１２０】

そして，制御部５０は，サーバ４に消去値およびクライアント名を送信する（図１０に図示せず）。消去値としては，クライアント５ｃの識別情報（たとえばＩＰアドレス等）に所定の演算（所定の方程式による演算，ハッシュ演算等）を施したものを使用することができるし，第１の実施の形態と同様にインデックス番号に所定の演算を施したもの，脱退要求送信の日時に所定の演算を施したもの等を使用することもできる。

【０１２１】

サーバ４は，消去値が正当かどうかを判断し，正当な場合には，加入者リスト

データベース４６の加入者リストから，消去値を送信したクライアント５ｃのリストセルを消去（削除）する（図１０に図示せず）。消去値が正当でない場合には，サーバ４は，消去値を送信したクライアント５ｃに警告等を発する（図１０に図示せず）。これにより，サーバ４は，データ配信サービスに加入している加入者を正確に把握することができるとともに，データ配信サービスの課金も適切に行うことができる。課金の方法は，前述した第１の実施の形態と同様にして行うことができる。

【０１２２】

なお，図１０に示すステップＳ８７およびＳ８９に示す送信をともにユニキャストにより行う場合には，暗号化グループセッション鍵Ｋｇｒｘおよび暗号化鍵更新鍵Ｋｕｘを１回の送信により，同時に送信することもできる。また，ステップＳ５３および／またはステップＳ５５において，クライアント３ｃが受信に成功しない場合には，サーバ４に再送要求を出し，サーバ４に再度送信させることもできる。

【０１２３】

また，一定の時間間隔Ｔ２（≠Ｔ１）で，データ配信サービスに加入しているクライアントとサーバ４とがユニキャスト通信を行い，その時有効なグループセッション鍵を，このグループセッション鍵とは相関関係のない他のグループセッション鍵に変更することもできる。これにより，データ配信サービスに加入していないクライアントが暗号化鍵Ｋｇｒを不正に入手した場合であっても，このクライアントがデータ配信サービスに関するデータを復号化することを防止できる。

【０１２４】

３．他の実施の形態

第１および第２の実施の形態におけるインターネット１はイントラネットであってもよい。

【０１２５】

また，第１のおよび第２の実施の形態において，コンテンツデータベース２４（４４）と加入者リストデータベース２５（４６）とは，同一のサーバではなく，別々のサーバにそれぞれ保持され，管理されていてもよい。この場合に，マル

チキャストグループ３（５）に属するクライアントは，加入者リストデータベース２５（４６）を保持するサーバ（加入者管理サーバ）に，データ配信サービスへの加入の登録を行い，コンテンツデータベース２４（４４）を保持するサーバ（データサーバ）からデータ配信サービスに関するデータを受信することとなる。サービスに加入したクライアントは，グループセッション鍵，鍵更新鍵等を，加入者管理サーバから受け取るようにすることもできるし，データサーバから受け取るようにすることもできる。同様にして，サービス料の課金は，加入者管理サーバが行ってもよいし，データサーバが行ってもよい。

【０１２６】

第１の実施の形態におけるサーバ２および配信データ受信装置３００の各処理は，ハードウェア回路によっても実現できるし，プログラムおよび該プログラムを実行するＣＰＵまたはマイクロコンピュータによっても実現できる。ただし，前述したように，配信データ受信装置３００の鍵復号鍵Ｋｍは，ハードウェア回路またはＩＣチップに形成されていることが好ましい。

【０１２７】

同様にして，第２の実施の形態におけるサーバ４およびクライアント５の各処理は，ハードウェア回路によっても実現できるし，プログラムおよび該プログラムを実行するＣＰＵまたはマイクロコンピュータによっても実現できる。

【０１２８】

（付記１）　所定のデータ配信サービスに関するデータをマルチキャストにより送信するマルチキャストサーバと，マルチキャストグループに属し，前記データを受信する複数のクライアントとを有するマルチキャスト通信システムであって，

前記マルチキャストサーバは，

前記データを第１の暗号化鍵により暗号化するデータ暗号部と，

前記データ暗号部により暗号化されたデータを，前記マルチキャストグループに属するクライアントにマルチキャストにより送信するデータ送信部と，

前記第１の暗号化鍵を第２の暗号化鍵により暗号化する鍵暗号部と，

前記鍵暗号部により暗号化された第１の暗号化鍵を，前記マルチキャストグル

ープに属するクライアントのうち，前記データ配信サービスに加入したクライアントにユニキャストにより送信する鍵送信部と，

を備え，

前記クライアントのうち，前記データ配信サービスに加入したクライアントは，

前記鍵送信部により送信される，暗号化された第１の暗号化鍵を受信する鍵受信部と，

前記鍵受信部により受信された，暗号化された第１の暗号化鍵を復号化鍵により復号化する鍵復号部と，

前記データ送信部により送信される，暗号化されたデータを，前記鍵復号部により得られた第１の暗号化鍵により復号するデータ復号部と，

を備えているマルチキャスト通信システム。

【０１２９】

（付記２）　付記１において，

前記マルチキャストサーバは，前記マルチキャストグループに属するクライアントのうち，前記データ配信サービスへの加入を希望するクライアントを登録する登録部をさらに備えているマルチキャスト通信システム。

【０１３０】

（付記３）　付記１または２において，

前記マルチキャストサーバが，前記データ配信サービスに加入したクライアントに対して，時間，または，受信したデータ量に応じた従量制の課金を行う課金部をさらに備えているマルチキャスト通信システム。

【０１３１】

（付記４）　付記２において，

前記マルチキャストサーバは，

前記登録部に登録されたクライアントから送信され，該クライアントが自己の保持する少なくとも前記第１の暗号化鍵を消去したことを示す消去データを受信する消去データ受信部と，

前記消去データ受信部により消去データが受信されると，該消去データを送信

したクライアントを前記登録部から抹消する抹消部と，

をさらに備え，

前記クライアントは，

前記データ配信サービスから脱退する場合には，自己が保持する少なくとも前記第１の暗号化鍵を消去する消去部と，

前記消去データを生成し，前記消去データを前記マルチキャストサーバに送信する消去データ送信部と，

をさらに備えているマルチキャスト通信システム。

【０１３２】

（付記５）　付記１から４のいずれか１つにおいて，

前記第２の暗号化鍵と前記復号化鍵とが同一の鍵であるマルチキャスト通信システム。

【０１３３】

（付記６）　付記５において，

前記第２の暗号化鍵および前記復号化鍵の双方は，前記データ配信サービスに加入したクライアントのそれぞれに個別に設けられた鍵である，マルチキャスト通信システム。

【０１３４】

（付記７）　付記５または６において，

前記復号化鍵がハードウェア回路または半導体チップにより構成されている，マルチキャスト通信システム。

【０１３５】

（付記８）　付記１から４のいずれか１つにおいて，

前記第２の暗号化鍵は，前記クライアントが前記第１の復号鍵を前記マルチキャストサーバの公開鍵により暗号化して該マルチキャストサーバに送信し，該マルチキャストサーバが自己の秘密鍵で復号化して得られる鍵である，

マルチキャスト通信システム。

【０１３６】

（付記９）　付記１から４のいずれか１つにおいて，

前記第２の暗号化鍵は，前記データ配信サービスに加入したクライアントに対して公開鍵基盤により発行されたディジタル証明書の公開鍵であり，

前記復号化鍵は，該ディジタル証明書の秘密鍵である，

マルチキャスト通信システム。

【０１３７】

（付記１０）　所定のデータ配信サービスに関するデータをマルチキャストにより送信するマルチキャストサーバと，マルチキャストグループに属し，前記データを受信する複数のクライアントのうち，前記データ配信サービスに加入したクライアントとの間で行われるマルチキャスト通信方法であって，

前記マルチキャストサーバは，前記データの暗号化に用いられる第１の暗号化鍵を第２の暗号化鍵により暗号化して，前記マルチキャストグループに属するクライアントのうち，前記データ配信サービスに加入したクライアントにユニキャストにより送信し，

前記クライアントは，前記ユニキャストにより送信される，暗号化された第１の暗号化鍵を受信すると，これを復号化鍵により復号化し，

前記マルチキャストサーバは，前記データを前記第１の暗号化鍵により暗号化して，前記マルチキャストグループに属するクライアントにマルチキャストにより送信し，

前記クライアントは，前記暗号化されたデータを受信すると，これを前記復号化鍵の復号化により得られた前記第１の暗号化鍵により復号化する，

マルチキャスト通信方法。

【０１３８】

（付記１１）　所定のデータ配信サービスに関するデータを第１の暗号化鍵により暗号化するデータ暗号部と，

前記データ暗号部により暗号化されたデータをマルチキャストにより，所定のマルチキャストグループに属するクライアントにマルチキャストにより送信するデータ送信部と，

前記第１の暗号化鍵を第２の暗号化鍵により暗号化する鍵暗号部と，

前記鍵暗号部により暗号化された第１の暗号化鍵を，前記マルチキャストに属

するクライアントのうち，前記データ配信サービスに加入したクライアントにユニキャストにより送信する鍵送信部と，

を備えているマルチキャストデータ送信装置。

【０１３９】

（付記１２）　所定のデータ配信サービスに関するデータをマルチキャストにより，所定のマルチキャストグループに属するクライアントに送信するマルチキャストデータ送信方法であって，

前記データの暗号化に用いられる第１の暗号化鍵を第２の暗号化鍵により暗号化して，前記マルチキャストグループに属するクライアントのうち，前記データ配信サービスに加入したクライアントにユニキャストにより送信し，

前記データを前記第１の暗号化鍵により暗号化して，マルチキャストにより前記マルチキャストグループに属するクライアントに送信する，

マルチキャストデータ送信方法。

【０１４０】

（付記１３）　マルチキャストにより送信される，所定のデータ配信サービスに関するデータを受信するマルチキャストデータ受信装置であって，

前記データ配信サービスに加入することにより得られる暗号化された第１の暗号化鍵を復号化する鍵復号部と，

前記データ配信サービスに関するデータが前記第１の暗号化鍵により暗号化されたものを受信するデータ受信部と，

前記データ受信部により受信された，暗号化されたデータを，前記鍵復号部の復号化により得られた第１の暗号化鍵により復号化するデータ復号部と，

を備えているマルチキャストデータ受信装置。

【０１４１】

（付記１４）　マルチキャストにより送信される，所定のデータ配信サービスに関するデータを受信するマルチキャストデータ受信方法であって，

前記データ配信サービスに加入することにより得られる暗号化された第１の暗号化鍵を復号化し，

前記データ配信サービスに関するデータが前記第１の暗号化鍵により暗号化さ

れたものを受信し，

前記受信した，暗号化されたデータを，前記復号化により得られた第１の暗号化鍵により復号化する，

マルチキャストデータ受信方法。

【０１４２】

（付記１５）　所定のデータ配信サービスに関するデータをマルチキャストにより送信するマルチキャストサーバと，マルチキャストグループに属し，前記データを受信する複数のクライアントとを有するマルチキャスト通信システムであって，

前記マルチキャストサーバは，

前記データを暗号化するためのデータ暗号化鍵を，所定の更新タイミングごとに，該更新タイミング前に有効なデータ暗号化鍵に，該更新タイミング前に有効なデータ暗号化鍵に対応する更新鍵を作用させることにより得られる関係にある，更新タイミング後に有効となるデータ暗号化鍵に更新する鍵更新部と，

前記更新鍵を生成し，または，あらかじめ保持する更新鍵保持部と，

前記データを現在有効なデータ暗号化鍵により暗号化するデータ暗号部と，

前記データ暗号部により暗号化されたデータを，前記マルチキャストグループに属するクライアントにマルチキャストにより送信するデータ送信部と，

前記更新タイミングごとに，更新タイミング後に有効なデータ暗号化鍵に対応する更新鍵を，該更新タイミング後に有効なデータ暗号化鍵により暗号化する鍵暗号部と，

前記更新タイミングごとに，前記鍵暗号部により暗号化された更新鍵を前記クライアントにユニキャストまたはマルチキャストにより送信する更新鍵送信部と，

を備え，

前記複数のクライアントのうち，前記データ配信サービスに加入したクライアントは，

前記データ送信部により送信される，暗号化されたデータを受信するデータ受信部と，

前記データ受信部により受信される，前記暗号化されたデータを，前記現在有効なデータ暗号化鍵と同一の現在有効なデータ復号化鍵により復号化するデータ復号部と，

前記更新鍵送信部により送信される，暗号化された更新鍵を受信する更新鍵受信部と，

前記更新鍵受信部により受信される，暗号化された更新鍵を，前記現在有効なデータ復号化鍵により復号化する更新鍵復号部と，

前記データ配信サービスへの加入時には，外部から与えられ，その後は，前記更新タイミングごとに，該更新タイミング前に有効なデータ復号化鍵に，該更新タイミング前に有効なデータ復号化鍵による復号化により得られた前記更新鍵を作用させることにより，更新タイミング後に有効なデータ復号化鍵を生成し，前記更新タイミングごとに，前記更新タイミング前に有効なデータ復号化鍵を前記更新タイミング後に有効なデータ復号化鍵に更新するデータ復号化鍵更新部と，

を備えているマルチキャスト通信システム。

【０１４３】

（付記１６）　所定のデータ配信サービスに関するデータをマルチキャストにより送信するマルチキャストサーバと，マルチキャストグループに属し，前記データを受信する複数のクライアントうち，前記所定のデータ配信サービスに加入したクライアントとを間で行われるマルチキャスト通信方法であって，

前記マルチキャストサーバは，前記データを現在有効なデータ暗号化鍵により暗号化して，前記マルチキャストグループに属するクライアントにマルチキャストにより送信し，

前記クライアントは，前記マルチキャストサーバから送信される，暗号化されたデータを受信して，前記暗号化されたデータを前記現在有効なデータ暗号化鍵と同一の現在有効なデータ復号化鍵により復号化し，

前記マルチキャストサーバは，前記データ暗号化鍵を，所定の更新タイミングごとに，該更新タイミング前に有効なデータ暗号化鍵に，該更新タイミング前に有効なデータ暗号化鍵に対応する更新鍵を作用させることにより得られる関係にある，更新タイミング後に有効となるデータ暗号化鍵に更新し，

前記マルチキャストサーバは，前記更新タイミングごとに，更新タイミング後に有効なデータ暗号化鍵に対応する更新鍵を，該更新タイミング後に有効なデータ暗号化鍵により暗号化して，前記クライアントにユニキャストまたはマルチキャストにより送信し，

前記クライアントは，前記マルチキャストサーバから送信される，暗号化された更新鍵を受信して，該暗号化された更新鍵を，前記現在有効なデータ復号化鍵により復号化し，

前記クライアントは，前記データ配信サービスへの加入時には，外部から与えられ，その後は，前記更新タイミングごとに，該更新タイミング前に有効なデータ復号化鍵に，該更新タイミング前に有効なデータ復号化鍵による復号化により得られた前記更新鍵を作用させることにより，更新タイミング後に有効なデータ復号化鍵を生成し，前記更新タイミングごとに，前記更新タイミング前に有効なデータ復号化鍵を前記更新タイミング後に有効なデータ復号化鍵に更新する，

マルチキャスト通信方法。

【０１４４】

（付記１７）　所定のデータ配信サービスに関するデータを暗号化するためのデータ暗号化鍵を，所定の更新タイミングごとに，該更新タイミング前に有効なデータ暗号化鍵に，該更新タイミング前に有効なデータ暗号化鍵に対応する更新鍵を作用させることにより得られる関係にある，更新タイミング後に有効となるデータ暗号化鍵に更新する鍵更新部と，

前記更新鍵を生成し，または，あらかじめ保持する更新鍵保持部と，

前記データを現在有効なデータ暗号化鍵により暗号化するデータ暗号部と，

前記データ暗号部により暗号化されたデータを，所定のマルチキャストグループに属するクライアントにマルチキャストにより送信するデータ送信部と，

前記更新タイミングごとに，更新タイミング後に有効なデータ暗号化鍵に対応する更新鍵を，該更新タイミング後に有効なデータ暗号化鍵により暗号化する鍵暗号部と，

前記更新タイミングごとに，前記鍵暗号部により暗号化された更新鍵を前記クライアントにユニキャストまたはマルチキャストにより送信する更新鍵送信部と

を備えているマルチキャストデータ送信装置。

【０１４５】

（付記１８）　所定のデータ配信サービスに関するデータをマルチキャストにより，所定のマルチキャストグループに属するクライアントに送信するマルチキャストデータ送信方法であって，

前記データを現在有効なデータ暗号化鍵により暗号化して，前記マルチキャストグループに属するクライアントにマルチキャストにより送信し，

前記データ暗号化鍵を，所定の更新タイミングごとに，該更新タイミング前に有効なデータ暗号化鍵に，該更新タイミング前に有効なデータ暗号化鍵に対応する更新鍵を作用させることにより得られる関係にある，更新タイミング後に有効となるデータ暗号化鍵に更新し，

前記更新タイミングごとに，更新タイミング後に有効なデータ暗号化鍵に対応する更新鍵を，該更新タイミング後に有効なデータ暗号化鍵により暗号化して，前記クライアントにユニキャストまたはマルチキャストにより送信する，

マルチキャストデータ送信方法。

【０１４６】

（付記１９）　マルチキャストサーバからマルチキャストにより送信される，所定のデータ配信サービスに関するデータを受信するマルチキャストデータ受信装置であって，

所定の更新タイミングごとに更新されるデータ暗号化鍵のうち，現在有効なデータ暗号化鍵によって，前記データが暗号化されたものを受信するデータ受信部と，

前記データ受信部により受信される，前記暗号化されたデータを，前記現在有効なデータ暗号化鍵と同一の現在有効なデータ復号化鍵により復号化するデータ復号部と，

前記データ復号化鍵を更新するために使用される更新鍵が前記現在有効なデータ暗号化鍵により暗号化されたものを前記マルチキャストサーバから受信する更新鍵受信部と，

前記更新鍵受信部により受信される，暗号化された前記更新鍵を，前記現在有効なデータ復号化鍵により復号化する更新鍵復号部と，

前記データ配信サービスへの加入時には，外部から与えられ，その後は，所定の更新タイミングごとに，該更新タイミング前に有効なデータ復号化鍵に，該更新タイミング前に有効なデータ復号化鍵による復号化により得られた前記更新鍵を作用させることにより，更新タイミング後に有効なデータ復号化鍵を生成し，前記更新タイミングごとに，前記更新タイミング前に有効なデータ復号化鍵を前記更新タイミング後に有効なデータ復号化鍵に更新するデータ復号化鍵更新部と，

を備えているマルチキャストデータ受信装置。

【０１４７】

（付記２０）　マルチキャストサーバからマルチキャストにより送信される，所定のデータ配信サービスに関するデータを受信するマルチキャストデータ受信方法であって，

所定の更新タイミングごとに更新されるデータ暗号化鍵のうち，現在有効なデータ暗号化鍵によって，前記データが暗号化されたものを受信し，

前記受信した，前記暗号化されたデータを，前記現在有効なデータ暗号化鍵と同一の現在有効な復号化鍵により復号化し，

前記データ復号化鍵を更新するために使用される更新鍵が前記現在有効なデータ暗号化鍵により暗号化されたものを前記マルチキャストサーバから受信し，

前記暗号化された前記更新鍵を，前記現在有効なデータ復号化鍵により復号化し，

前記データ配信サービスへの加入時には，外部から与えられ，その後は，所定の更新タイミングごとに，該更新タイミング前に有効なデータ復号化鍵に，該更新タイミング前に有効なデータ復号化鍵による復号化により得られた前記更新鍵を作用させることにより，更新タイミング後に有効なデータ復号化鍵を生成し，前記更新タイミングごとに，前記更新タイミング前に有効なデータ復号化鍵を前記更新タイミング後に有効なデータ復号化鍵に更新する，

マルチキャストデータ受信方法。

【０１４８】

【発明の効果】

本発明によると，マルチキャスト通信において，データの暗号化を適切に行うことができる。また，本発明によると，マルチキャストサーバまたはデータ配信サービスの加入者を管理するサーバは，マルチキャストグループに属するクライアントのうち，データ配信サービスに加入しているクライアントを把握できる。さらに，本発明によると，加入から脱退時までのデータ受信量に応じた課金を行ったり，あるいは，加入から脱退までの時間に応じた課金を行うことにより，木目の細かい従量制課金を行うことができる。

【図面の簡単な説明】

【図１】

本発明の第１の実施の形態によるマルチキャスト通信システムの全体構成を示すブロック図である。

【図２】

第１の実施の形態によるマルチキャストサーバの構成を示すブロック図である。

【図３】

加入者リストのデータ構造を示す。

【図４】

配信データ受信装置（またはアダプタ）の構成を示すブロック図である。

【図５】

第１の実施の形態によるサーバおよびマルチキャストグループに属するクライアントの処理の流れを示すシーケンス図である。

【図６】

本発明の第２の実施の形態によるマルチキャスト通信システムの全体構成を示すブロック図である。

【図７】

第２の実施の形態によるマルチキャストサーバの構成を示すブロック図である。

【図８】

複数のグループセッション鍵と，各グループセッション鍵に対応する鍵更新鍵とが対になった鍵データを示す。

【図９】

第２の実施の形態によるクライアントの構成を示すブロック図である。

【図１０】

第２の実施の形態によるサーバおよびマルチキャストグループに属するクライアントの処理の流れを示すシーケンス図である。

【符号の説明】

１　インターネット

２，４　マルチキャストサーバ

３，５　マルチキャストグループ

３ａ～３ｄ，５ａ～５ｄ　クライアント

２０，３０，４０，５０　制御部

２１，４１　データ暗号部

２２，４２　鍵暗号部

２３，３１，４３，５１　送受信部

２４，４４　コンテンツデータベース

２５，４６　加入者リストデータベース

４５　鍵データベース

３００　配信データ受信装置

３２　データ復号部

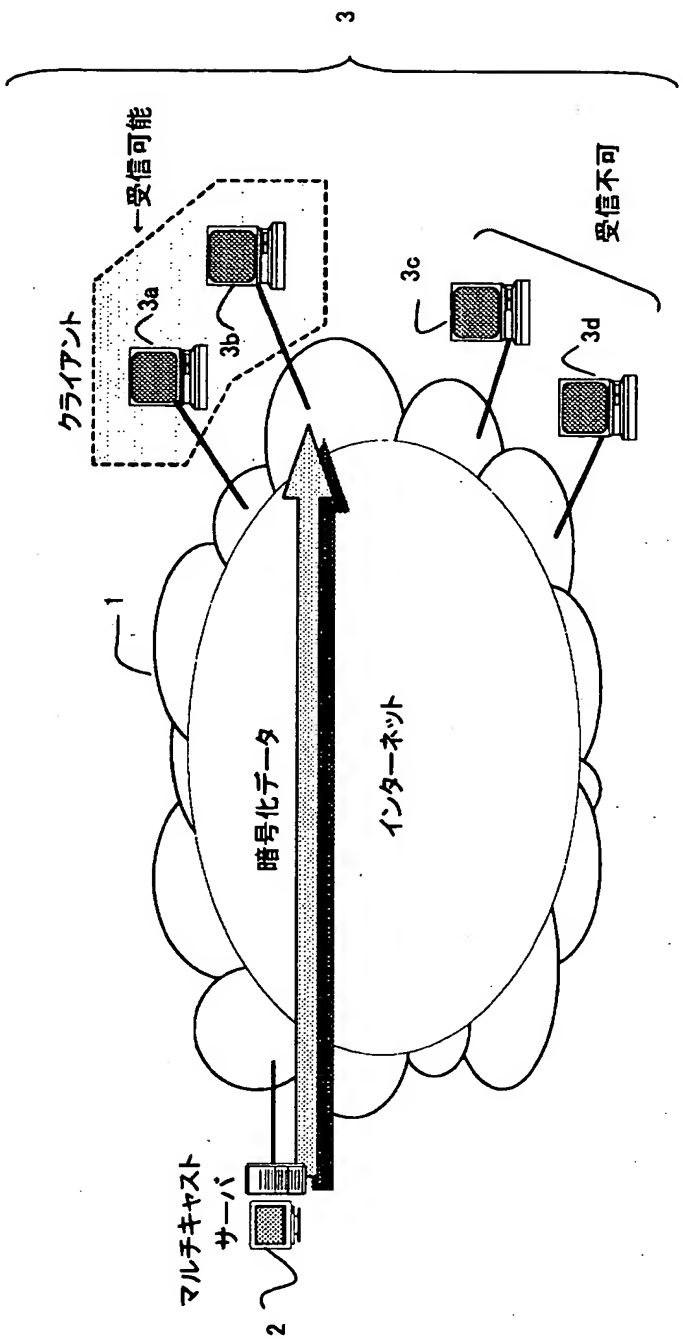
３３，５３　鍵復号部

３４　鍵復号鍵保持部

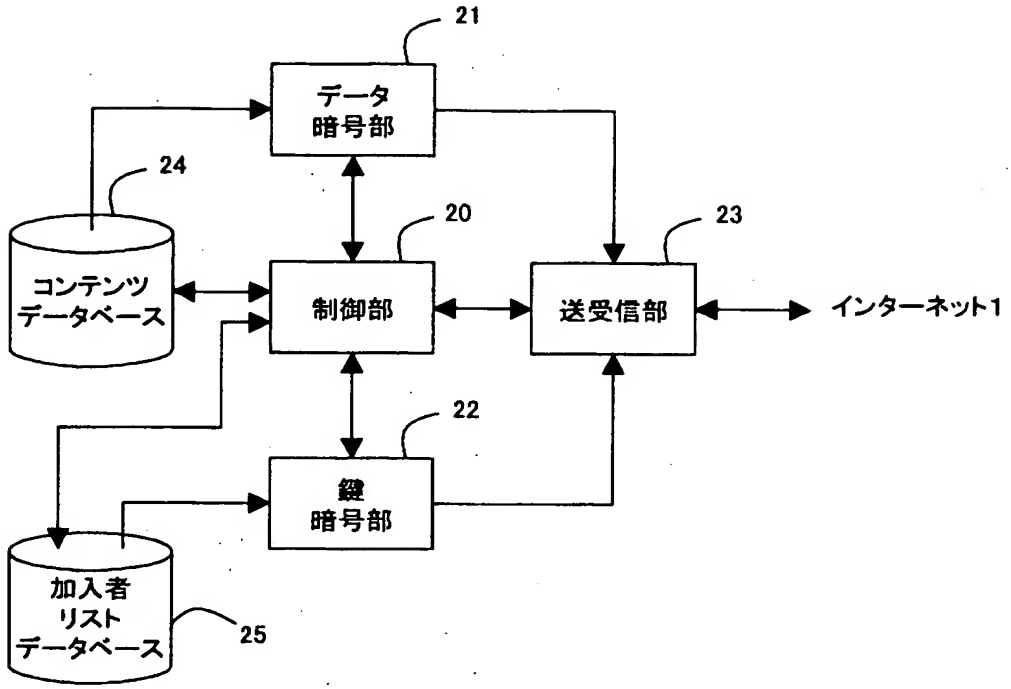
５６　鍵生成部

【書類名】　　図面

【図１】



【図２】

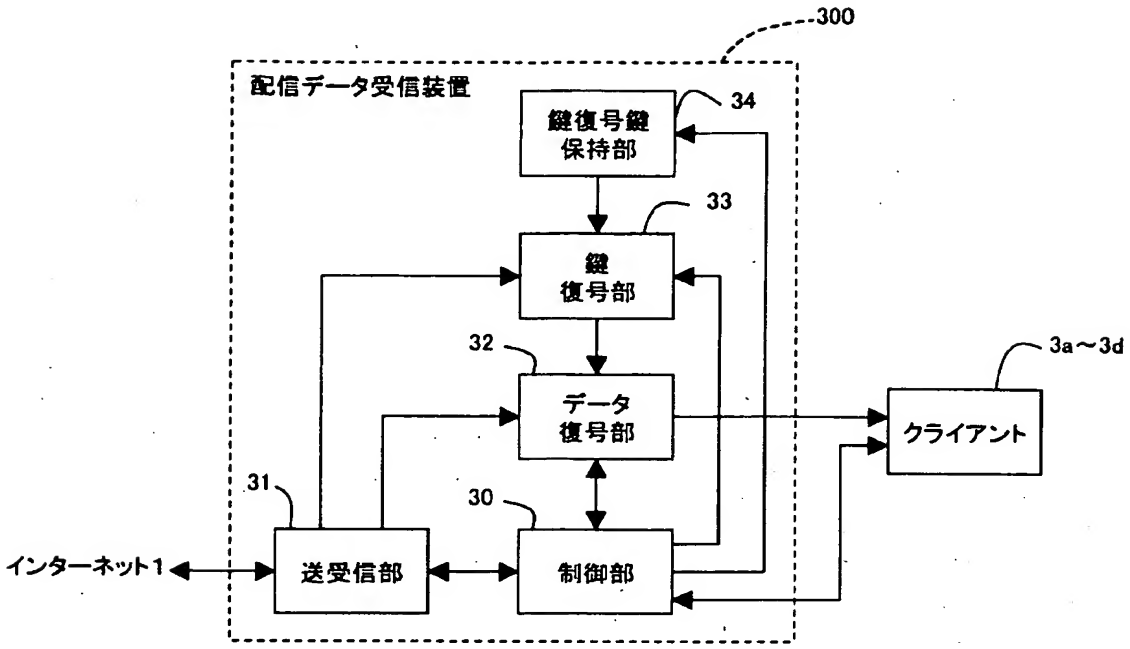


【図３】

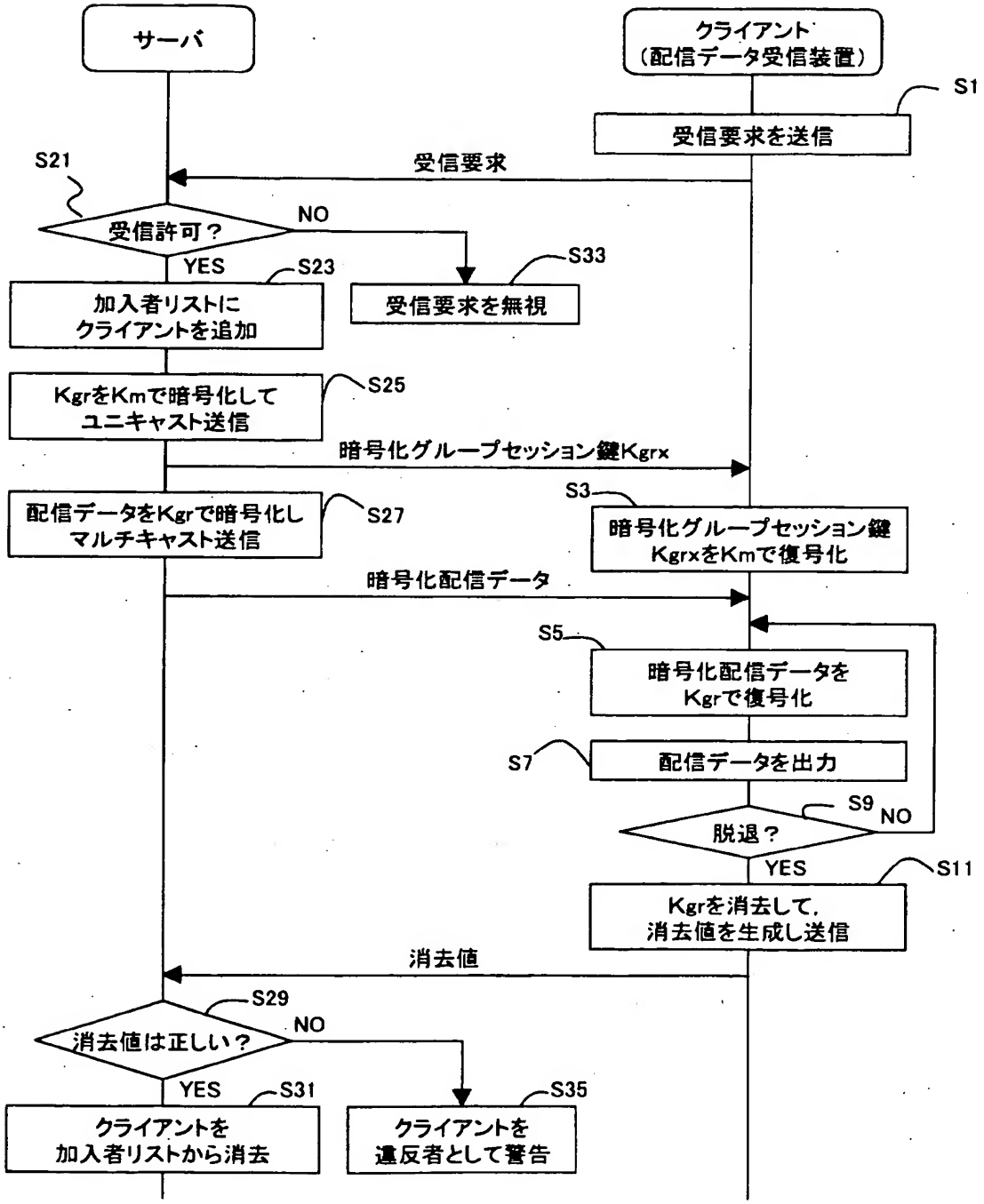
加入者リスト

加入者名	鍵復号鍵	加入日時
クライアントA	Km(A)	T(A)
クライアントB	Km(B)	T(B)
・ ・ ・	・ ・ ・	・ ・ ・

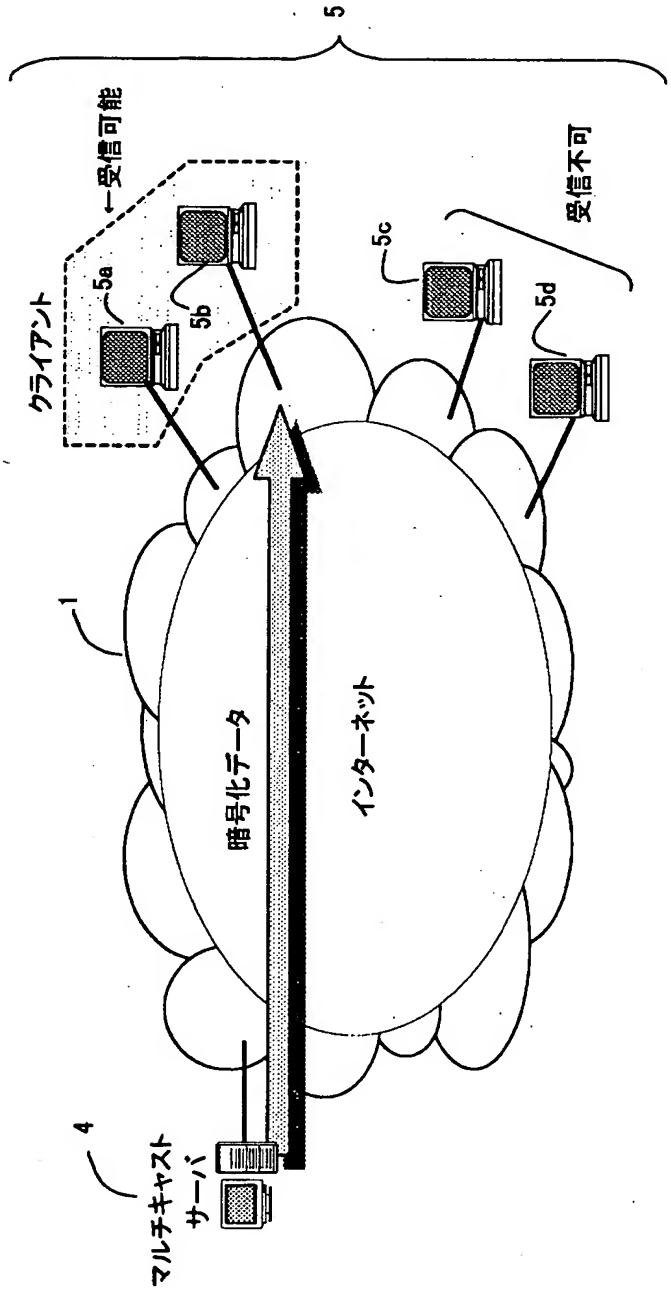
【図４】


300
配信データ受信装置
鍵復号鍵
保持部
34
33
鍵
復号部
32
データ
復号部
3a～3d
クライアント
31
30
インターネット1
送受信部
制御部

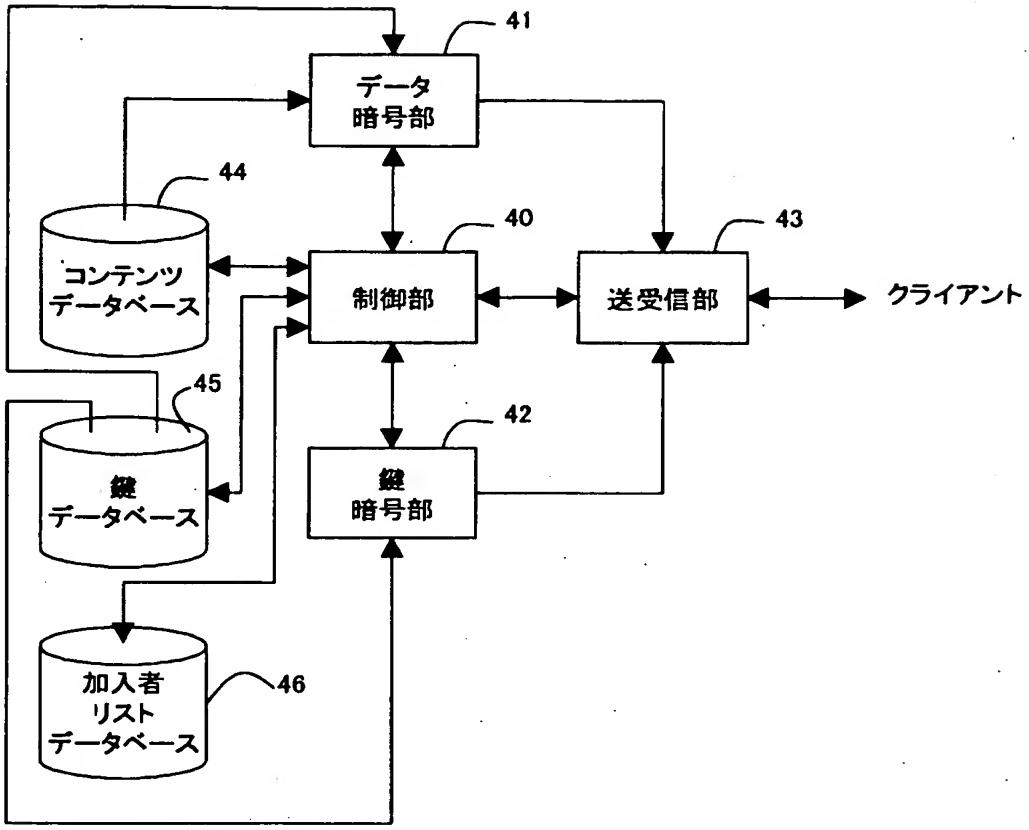
【図５】


サーバ
クライアント
（配信データ受信装置）
S1
受信要求を送信
S21
受信要求
受信許可？
NO
YES
S23
S33
加入者リストに
クライアントを追加
受信要求を無視
KgrをKmで暗号化して
ユニキャスト送信
S25
暗号化グループセッション鍵Kgrx
配信データをKgrで暗号化し
マルチキャスト送信
S27
S3
暗号化グループセッション鍵
KgrxをKmで復号化
暗号化配信データ
S5
暗号化配信データを
Kgrで復号化
S7
配信データを出力
S9
NO
脱退？
YES
S11
Kgrを消去して，
消去値を生成し送信
消去値
S29
消去値は正しい？
NO
YES
S31
S35
クライアントを
加入者リストから消去
クライアントを
違反者として警告

【図６】



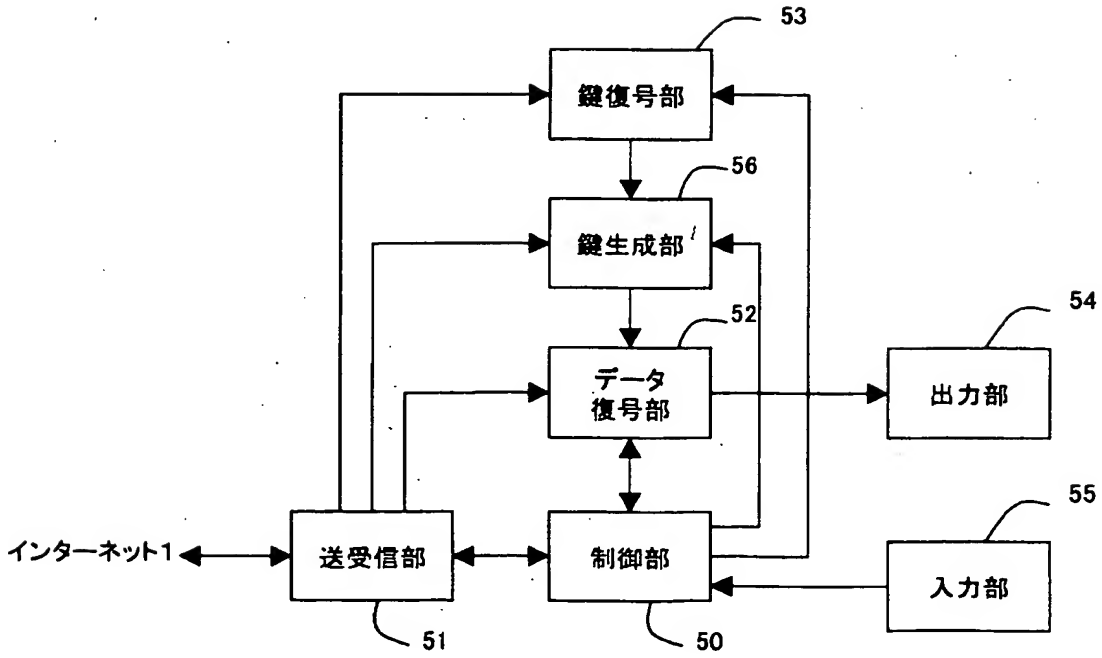
【図７】


41
データ
暗号部
44
コンテンツ
データベース
40
制御部
43
送受信部
クライアント
45
鍵
データベース
42
鍵
暗号部
加入者
リスト
データベース
46

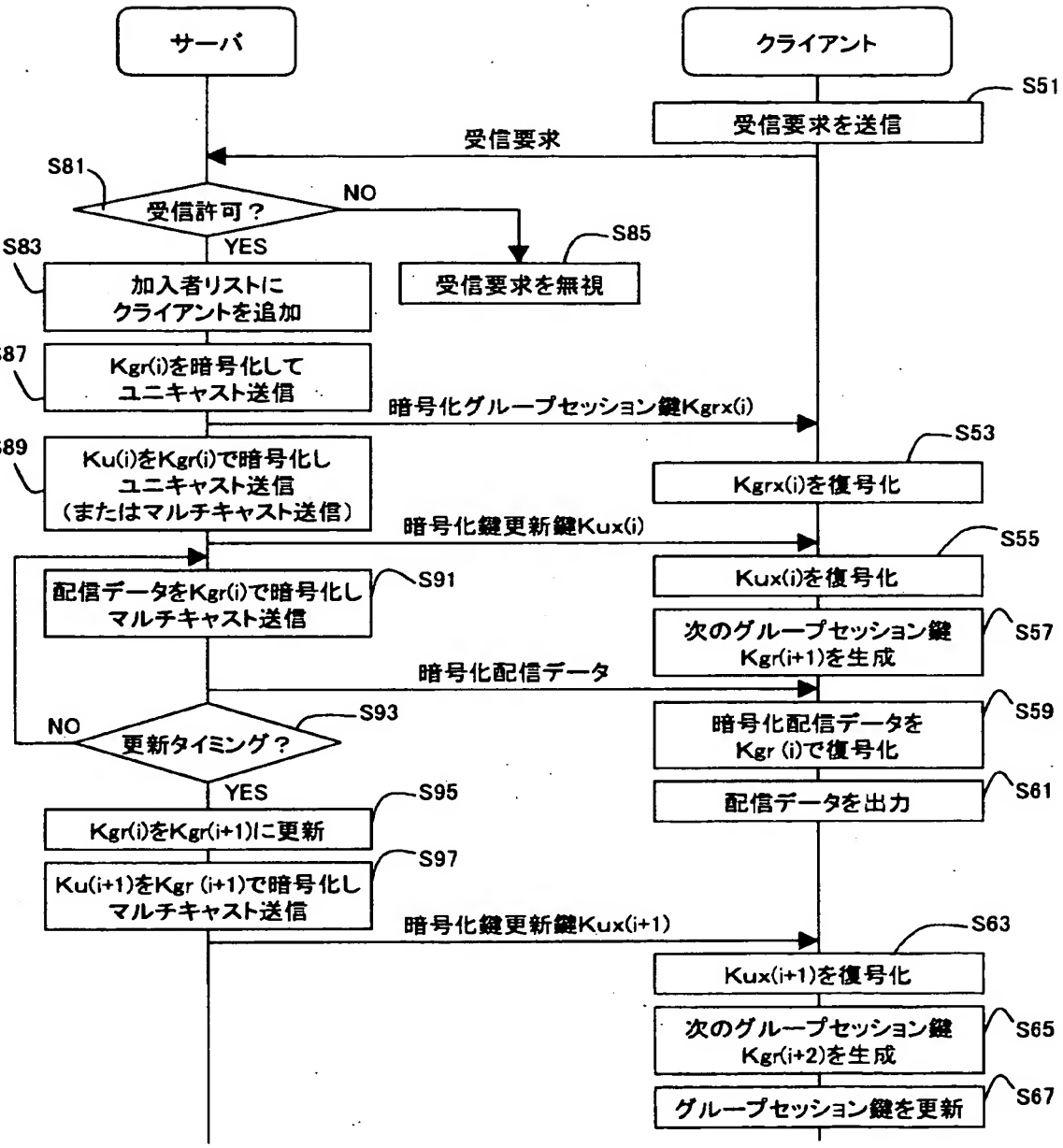
【図８】

グループセッション鍵	鍵更新鍵
Kgr (1)	Ku (1)
Kgr (2)	Ku (2)
Kgr (3)	Ku (3)
・ ・ ・	・ ・ ・
Kgr (i)	Ku (i)
Kgr (i+1)	Ku (i+1)
・ ・ ・	・ ・ ・

【図９】



【図１０】


サーバ
クライアント
S51
受信要求を送信
受信要求
S81
受信許可？
NO
S85
受信要求を無視
YES
S83
加入者リストに
クライアントを追加
S87
Kgr(i)を暗号化して
ユニキャスト送信
暗号化グループセッション鍵Kgrx(i)
S89
Ku(i)をKgr(i)で暗号化し
ユニキャスト送信
（またはマルチキャスト送信）
S53
Kgrx(i)を復号化
暗号化鍵更新鍵Kux(i)
S55
Kux(i)を復号化
S91
配信データをKgr(i)で暗号化し
マルチキャスト送信
次のグループセッション鍵
Kgr(i+1)を生成
S57
暗号化配信データ
S59
暗号化配信データを
Kgr (i)で復号化
S93
NO
更新タイミング？
YES
S61
配信データを出力
S95
Kgr(i)をKgr(i+1)に更新
S97
Ku(i+1)をKgr (i+1)で暗号化し
マルチキャスト送信
暗号化鍵更新鍵Kux(i+1)
S63
Kux(i+1)を復号化
次のグループセッション鍵
Kgr(i+2)を生成
S65
グループセッション鍵を更新
S67

【書類名】　　要約書

【要約】

【課題】　マルチキャスト通信において暗号化を適切に行う。

【解決手段】　マルチキャストサーバ２は，データ配信サービスに関するデータの暗号化に用いられるグループセッション鍵Ｋgrを第２の暗号化鍵Ｋｍにより暗号化して，マルチキャストグループ３に属するクライアントのうち，該サービスに加入したクライアントにユニキャストにより送信する。該サービスに加入したクライアントは，ユニキャストにより送信される，暗号化された第１の暗号化鍵を受信すると，これを復号化鍵Ｋｍにより復号化する。続いて，マルチキャストサーバ２は，データを第１の暗号化鍵により暗号化して，マルチキャストグループ３に属するクライアントにマルチキャストにより送信する。クライアントは，暗号化されたデータを受信すると，これを復号化鍵の復号化により得られた第１の暗号化鍵により復号化する。

【選択図】　　図５

認定・付加情報

特許出願の番号	特願２００１－２５８８９０
受付番号	５０１０１２６０２３７
書類名	特許願
担当官	佐藤　一博　　１９０９
作成日	平成１３年　９月　４日

＜認定情報・付加情報＞

【特許出願人】

【識別番号】	000005223
【住所又は居所】	神奈川県川崎市中原区上小田中４丁目１番１号
【氏名又は名称】	富士通株式会社

【代理人】　申請人

【識別番号】	100094514
【住所又は居所】	神奈川県横浜市港北区新横浜３－９－５　第三東昇ビル３階　林・土井　国際特許事務所
【氏名又は名称】	林　恒徳

【代理人】

【識別番号】	100094525
【住所又は居所】	神奈川県横浜市港北区新横浜３－９－５　第三東昇ビル３階　林・土井　国際特許事務所
【氏名又は名称】	土井　健二

次頁無

出　願　人　履　歴　情　報

識別番号　　〔０００００５２２３〕

１．変更年月日　　１９９６年　３月２６日
［変更理由］　住所変更
住　所　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　富士通株式会社